



8-18-04

AF/2635

120

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of: <b>Joseph R. Goetz</b>	Date: <b>16 August 2004</b>
Serial Number: <b>09/834,499</b>	Group Art Unit: <b>2635</b>
Filed: <b>12 April 2004</b>	Examiner: <b>Au, Scott D.</b>
For: <b>"AUTOMATIC VEHICLE THEFT PROTECTION SYSTEM"</b>	Attorney Docket No.: <b>7891-A-2</b>

## CERTIFICATE OF MAILING UNDER 37 CFR 1.8

RECEIVED

Mail Stop Appeal Brief - Patent  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

AUG 19 2004

Technology Center 2600

Dear Sir:

I hereby certify that this correspondence, consisting of this Certificate of Mailing, Appellant's Brief, in triplicate, a check in the amount of \$165.00 for Brief Filing Fees, and a Postcard is being deposited in the United States Postal Service as Express Mail in an envelope addressed to:

Mail Stop Appeal Brief - Patent  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

on

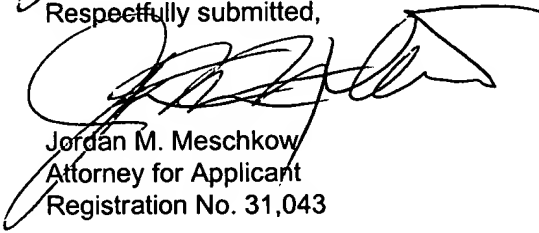
16 August 2004  
Date

16 August 2004

MESCHKOW & GRESHAM, P.L.C.  
5727 North Seventh Street  
Suite 409  
Phoenix, Arizona 85014  
602-274-6996

  
Signature

Respectfully submitted,

  
Jordan M. Meschkow  
Attorney for Applicant  
Registration No. 31,043



In re the Application of: <b>Joseph R. Goetz</b>	Date: <b>16 August 2004</b>
Serial Number: <b>09/834,499</b>	Group Art Unit: <b>2635</b>
Filed: <b>12 April 2001</b>	Examiner: <b>Au, Scott D.</b>
Title: <b>"Automatic Vehicle Theft Protection System"</b>	Attorney Docket No: <b>7891-A-2</b>

Assistant Commissioner For Patents  
Washington, D.C. 20231

**RECEIVED**

AUG 19 2004

**APPELLANT'S BRIEF**

Technology Center 2600

Dear Sir:

This Brief is filed pursuant to a Notice of Appeal mailed on 21 June 2004 in the matter of the above-identified application.

**(1) Real Party In Interest**

Joseph R. Goetz is the real party in interest of this application.

**(2) Related Appeals And Interferences**

Appellant is aware of no related application that will directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal.

**(3) Status Of Claims**

Claims 1-20 are on appeal. APPENDIX I provides a clean copy of the claims on appeal.

Claims 1, 3-4, and 8-9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Iijima et al.*, U.S. Pat. No. 5,708,307 (hereinafter *Iijima*) in view of *Takagi et al.*, U.S.

165.00 OP

01 FC:2402

08/19/2004 HAL111 00000040 09834499

Pat. No. 6,285,948 (hereinafter *Takagi*).

Claim 2 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* as applied to claim 1, and further in view of *Tuttle* (U.S. Pat. No. 6,112,152).

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* as applied to claim 4, and further in view of *Tallman et al.* (U.S. Pat. No. 6,175,308).

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* as applied to claim 4, and further in view of *Bethards* (U.S. Pat. No. 5,040,212).

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* as applied to claim 4, and further in view of *Strohbeck* (U.S. Pat. No. 6,580,972).

Claim 10 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* as applied to claim 1, and further in view of *Weber* (U.S. Pat. No. 3,784,839).

Claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and *Weber* as applied to claim 10, and further in view of *Flanagan* (U.S. Pat. No. 3,864,651).

Claim 12 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*, *Weber*, and *Flanagan* as applied to claim 11, and further in view of *Hansen* (U.S. Pat. No. 4,412,267).

Claim 13 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*, *Weber*, and *Flanagan* as applied to claim 11, and further in view of *Dodd et al.* (U.S. Pat. No. 5,313,189).

Claim 14 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* as applied to claim

1, and further in view of *Bryant et al.* (U.S. Pat. No. 5,155,494).

Claim 15 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*.

Claim 16 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Tallman*.

Claim 17 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Strohbeck*.

Claim 18 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*.

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Bryant*.

Claim 20 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*, *Weber*, *Flanagan*, *Hansen*, *Dodd*, and *Bryant*.

APPENDIX II provides copies of the *Iijima*, *Takagi*, *Tuttle*, *Tallman*, *Bethards*, *Strohbeck*, *Weber*, *Flanagan*, *Hansen*, *Dodd*, and *Bryant* references.

#### **(4) Status Of Amendments**

No amendments have been filed subsequent to final rejection.



**(5) Summary Of Invention**

Referring to FIG. 2, and Appellant's specification at page 5, line 22, through page 14, line 21, FIG. 2 shows a block diagram of an automatic vehicle theft prevention system 52 interconnected in series between an ignition key switch 32 and a starter motor 34 of an ignition system of a motor vehicle.

The vehicle theft prevention system 52 includes an interrogator circuit 54, in radio communication with a transponder circuit 56. A controller 58, in communication with the interrogator circuit 54, is configured to selectively actuate an enable relay 62, and the enable relay 62, in turn, actuates a latching relay 64. In addition, an override switch 60 is coupled to an input of the latching relay 64.

The interrogator circuit 54 includes a signal generator 66 that generates an excitation signal 68 and an antenna 70 coupled to the signal generator 66 for radiating the excitation signal 68. The system 52 relies on proximity sensing. Thus, the antenna 70 is configured for placement inside passenger compartment 24 of motor vehicle 20 preferably close to the driver side seat. The override switch 60 and an override indicator 92 are also located inside the passenger compartment of the motor vehicle.

The transponder circuit 56 is a mobile RFID data carrier that includes a memory element 78 containing an identification code 76 and a transceiver. The transponder circuit 56 is externally powered and derives its power from the excitation signal 68, radiated from the interrogator circuit 54. The transponder circuit 56 is separate from the vehicle's ignition key so that a

thief having access to the vehicle's key, but not having access to transponder circuit 56, cannot start the vehicle's engine.

The controller 58 includes an input for receiving a predetermined authorized identification code 96 from an external programming device 98. A memory element 100 of the controller 58 is in communication with the input for storing the predetermined authorized identification code 96. The input may be a data port 102 configured for a wired interconnection 104 with programming device 98, or alternatively, the programming device 98 may be a wireless transmitter, and the input is the antenna 70 configured for radio frequency communication with the programming device 98 over a wireless communication link 106. The predetermined authorized identification code 96 corresponds to the identification code 76. As such, the controller 58 is programmed to recognize the identification code 76 for the transponder circuit 56 and actuate system 52 in response to the identification code.

The system 52 may be actuated by more than one transponder circuit. For example, the system 52 includes a second RFID data carrier transponder circuit 108, separate from the vehicle's key 48. The second RFID data carrier 108, has a memory element 110 for storing a second identification code 112. A second predetermined authorized identification code 114, corresponding to second identification code 112, is received at the input of controller 58 and stored in memory element 100.

In operation, the system 52 is initially set to a disable mode so that the ignition system cannot be enabled and the vehicle engine cannot be started. The system 52 is maintained

in this disable mode whenever controller 58 fails to detect either of the identification codes 76 and 112. In order to operate the motor vehicle, the driver moves in proximity to the antenna 70 of the interrogator circuit 54 carrying one of transponder circuits 56 and 108.

The transponder circuit 56 detects and modulates the excitation signal 68 radiated by the antenna 70 to produce a return signal 74 for receipt at the antenna 70. The return signal 74 contains one of the identification codes 76 and 112 identifying the transponder circuit 56 or 108. The controller 58 then attempts to match the received identification code within the return signal 74 with one of the predetermined authorized identification codes 96 and 114. When the controller 58 detects a match, controller 58 actuates the enable relay 62 to a momentary closed state. In response to the momentary actuation of the enable relay 62, the latching relay 64 is also actuated to a latched, or closed, state.

A circuit path is thus formed from ignition switch output to the input of starter motor 34. This circuit path allows system 52 to be in the enable mode so that when the vehicle ignition key is inserted into the ignition switch 32 and turned, the vehicle engine may be started. Whenever the ignition switch is turned off using the vehicle key, the latching relay 64 opens and the automatic vehicle theft prevention system 52 is placed back into the disable mode.

When the driver wishes to override the system 52, it is incumbent upon the driver to activate the override switch 60 which causes latching relay 64 to remain latched, following

actuation of latching relay 64 until the system 52 is no longer bypassed by driver deactivation of the override switch 60. In addition, activation of override switch 60 energizes indicator 92 to provide visual or audible indication to the driver that override switch 60 is activated.

**(6) Issues**

The following issues are presented for review:

1. Whether claims 1, 3-4, and 8-9 are unpatentable under 35 U.S.C. §103(a) over *Iijima* (U.S. Pat. No. 5,708,307) in view of *Takagi* (U.S. Pat. No. 6,285,948).
2. Whether claim 2 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Tuttle* (U.S. Pat. No. 6,112,152).
3. Whether claim 5 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Tallman et al.* (U.S. Pat. No. 6,175,308).
4. Whether claim 6 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Bethards* (U.S. Pat. No. 5,040,212).
5. Whether claim 7 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Strohbeck* (U.S. Pat. No. 6,580,972).
6. Whether claim 10 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Weber* (U.S. Pat. No. 3,784,839).
7. Whether claim 11 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Flanagan* (U.S. Pat. No. 3,864,651).
8. Whether claim 12 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi*, *Weber*, and *Flanagan* and further in view of *Hansen* (U.S. Pat. No. 4,412,267).

9. Whether claim 13 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi*, *Weber*, and *Flanagan* and further in view of *Dodd et al.* (U.S. Pat. No. 5,313,189).
10. Whether claim 14 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Bryant et al.* (U.S. Pat. No. 5,155,494).
11. Whether claim 15 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi*.
12. Whether claim 16 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Tallman*.
13. Whether claim 17 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Strohbeck*.
14. Whether claim 18 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi*.
15. Whether claim 19 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Bryant*.
16. Whether claim 20 is unpatentable under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi*, *Weber*, *Flanagan*, *Hansen*, *Dodd*, and *Bryant*.

#### (7) Grouping Of Claims

It is Appellant's position that claim 1, 15, and 18 are separately patentable from all other claims on appeal.

It is Appellant's position that claim 6 is separately patentable from all other claims on appeal.

It is Appellant's position that claims 2-5, 7-14, 16-17, and 19-20 stand or fall together and are separately patentable from claims 1, 6, 15, and 18.

(8) Argument

Group 1, Claim 1

A First Office Action dated 6 November 2003 rejected claim 1 under 35 U.S.C. 103(a) as being unpatentable over *Iijima* (U.S. Pat. No. 5,708,307) in view of *Takagi* (U.S. Pat. No. 6,285,948). Claim 15 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*. Claim 18 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*. In response to the 6 November 2003 Office Action, Appellant filed a Response on 5 January 2004. A Second Non-final Office Action dated 30 March 2004 maintains the rejection.

*Iijima* teaches of an anti-theft car protection system that includes a transmitter-receiver for receiving a code of a specialized key, the key having a transponder built therein. The transponder includes an EEPROM for storing an ID number of the key. When the *Iijima* receives a code of the key, an immobilizer unit compares the code as received with a code as registered. When the codes coincide, the immobilizer unit transmits an engine start permission signal to an engine control unit so that the engine is enabled to start.

*Takagi* teaches of an engine control apparatus, in which a control program is stored in a non-volatile rewritable memory. The control program may be rewritten by a rewriting tool following 1) a match between a key identification code from a vehicle key and a key reference code stored in the non-volatile rewritable memory, and 2) a match between a program

identification code from the rewriting tool and a program reference code stored in the non-volatile rewritable memory. *Takagi* further teaches that the vehicle key is an electronic-type key which is provided with a transponder that includes a key identification code exclusive to the key. However, *Takagi* explains that the transponder may alternatively be provided separately from the key.

The 6 November 2003 First Office Action alleged that *Iijima* teaches the limitations recited in independent claim 1 of the above-identified application, except for the transponder circuit being separate from the ignition key for detecting the excitation signal and radiating the return signal. However, the First Office Action further alleged that *Takagi* teaches of a transponder circuit separate from the ignition key. The First Office Action concluded that it would have been obvious to separate the transponder circuit from the ignition key, as disclosed by *Takagi*, into the system of *Iijima* because "*Takagi et al.* teach separating the transponder from the key as an alternative to combining the two in order to achieve the same end result."

The 5 January 2004 Response filed by Appellant argued that it was improper to combine the teachings of *Iijima* and *Takagi* to render obvious Applicant's invention of independent claim 1 because 1) *Iijima* would be rendered unworkable for its intended purpose, and 2) the *Iijima* system utilizing a specialized key, necessary to the invention of *Iijima*, suffers from the very problems Applicant's invention of claim 1 corrects.

The 30 March 2004 Second Non-final Office Action found

Appellant's argument non-persuasive. In particular, the Second Non-final Office Action acknowledges that references cannot be arbitrarily combined, but that there must be some reason why one skilled in the art would be motivated to make the proposed combination of primary and secondary references. The Second Office Action argues that there is no requirement that a motivation to make the modification be expressly articulated. Rather, the test for combining references is what the combination of disclosures taken as a whole would suggest to one of ordinary skill in the art. The Second Office Action concludes that it would have been obvious to separate the transponder circuit from the ignition key because *Takagi* teach separating the transponder from the key as an alternative to combining the two in order to achieve the same end result.

It is Appellant's position that invention is to be gauged not only by the extent or simplicity of the physical changes, but also by the perception of the necessity or desirability of making such changes to produce a new result.

The Background of the Invention section of Applicant's specification details several problems associated with prior art transponder-based immobilizer systems, such as that taught by *Iijima*. Most specifically, when the transponder is embedded on the key, the vehicle owner cannot readily have a duplicate key made. Rather, the vehicle owner is required to obtain duplicate keys through the vehicle dealer or through an authorized provider, which is inconvenient for the vehicle owner and significantly more expensive than merely having a duplicate key made at a local hardware store. In addition, if the key with the embedded transponder is stolen, such as in a home robbery



where the thief finds the vehicle keys setting in the home or in a car jacking in which the thief takes the key from the driver, the thief can still start the car. Yet another problem arises with these prior art systems in that they are only provided in new vehicles, and cannot be readily adapted for use with older model vehicles, collectable vehicles, a fleet of vehicles, and such.

As stated in In re Bisley, 94 USPQ 80, 86-87 (C.C.P.A. 1952):

Moreover, the conception of a new and useful improvement must be considered along with the actual means of achieving it in determining the presence or absence of invention....The discovery of a problem calling for an improvement is often a very essential element in an invention correcting such a problem; and though the problem, once realized, may be solved by use of old and known elements, this does not necessarily negative invention.

Appellant's invention of claim 1 including a transponder circuit separate from the ignition key for detecting the excitation signal and radiating the return signal is not a mere arbitrary design choice. Rather, it is the cooperative relationship of the claimed elements that achieves a novel and unobvious benefit for Applicant's invention of cost savings when obtaining duplicate keys; enhanced anti-theft capability; and ready incorporation into older model vehicles, collectable vehicles, a fleet of vehicles, and such.

*Iijima* fails to expressly articulate a motivation for making the modification suggested by the Examiner. In addition, *Iijima* fails to impliedly suggest any motivation for separating the transponder from the key in the *Iijima* system as proposed by the

Examiner. To do so would alter the construction and mode of operation of the *Iijima* anti-theft car protection system, which ensures start of the engine without repetition of key operation and inconvenience regarding the anti-theft protection system as long as the key as applied is a formal one (col. 1, line 66, through col. 2, line 4), so that it would not function in its intended manner. *Iijima* requires this specialized key (i.e., formal key) to prevent car theft by shape forgery of the mechanical key. Accordingly, separation of the transponder from the key is contrary to the express purpose of the *Iijima* system. Consequently, it appears that the obviousness of the proposed change is not derived from the cited prior art, but only from Appellant's disclosure.

Well established patent practice dictates that there must be some suggestion or incentive in the prior art to combine the teachings of the prior art. Absent this suggestion or incentive, the combination is improper. The *Iijima* system utilizing a specialized key, necessary to the invention of *Iijima*, suffers from the very problems Appellant's invention of claim 1 corrects. Moreover, since *Iijima* would be rendered unworkable for its intended purpose, *Iijima* cannot suggest, either expressly or impliedly, the desirability of modifications which make the *Iijima* anti-theft car protection system more closely resemble Applicant's invention of claim 1, notwithstanding the teachings of the *Takagi* reference.

For the reasons set forth above, the rejection of claim 1 under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* was improper. Independent claims 15 and 18 include the above discussed limitations of claim 1. As such,

the rejections of claims 15 and 18 as being unpatentable over *Iijima* in view of *Takagi* are improper for the reasons set forth above in connection with claim 1. Accordingly, the Board is respectfully requested to reverse the rejection of claim 1, 15, and 18 under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*.

**Group 2, Claim 6**

The Second Non-final Office Action rejected claim 6 under 35 U.S.C. §103(a) over *Iijima* in view of *Takagi* and further in view of *Bethards*. *Bethards* teaches of methodology for programming a communication device (i.e., a subscriber unit) to recognize voice commands. In particular, a portable programming apparatus is employed to transmit data (in this case an identified codebook) for receipt at an antenna (62) of a subscriber unit (14), which stores the codebook. Thereafter, the subscriber unit may response to the voice commands.

The Office Action alleges that it would have been obvious to include an antenna configured for radio frequency communication of codebook data disclosed by *Bethards* into the controller device of *Iijima* and *Takagi* "with the motivation for doing so would allow the preset code in the controller is used to communicate with the transponder to operate the vehicle system."

It's Appellant's position that it is not obvious to modify a hypothetical combination of *Iijima* and *Takagi* to include radio frequency communication capability via an external programming device, to render obvious Appellant's invention of claim 6. As stated in In re Fritch, 23 USPQ 2d 178-, 1783-84 (Fed. Cir. 1992):

"Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined only if there is some suggestion or incentive to do so." (quoting *ACS Hosp. Systems, Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984))....The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification.

*Iijima* and *Takagi* do not suggest the desirability of modifying the theoretical combination of *Iijima* and *Takagi* *Yamashita* mobile communication system to include radio frequency communication capability via an external programming device. Indeed, no motivation is provided for such a modification because *Takagi* already includes means for providing a providing a predetermined authorized access code via a wired connection.

*Takagi* explicitly discloses an external programming device (i.e., a rewriting tool 14) that physically couples to the electronic control unit 2 via a connector 34 (see FIG. 1 and col. 3, lines 5-8). *Takagi* further explicitly discloses that the key ID is stored in the electronic control unit and is rewritable. Thus, the key ID can be changed to a new one, if the key is stolen (see col. 6, lines 10-14). To modify the hypothetical combination of *Iijima* and *Takagi* to include radio frequency communication capability via an external programming device, such as that taught by *Bethards*, would be redundant, therefore an unnecessary and costly modification.

For the reasons set forth above, there is no suggestion or incentive to combine the teachings of *Iijima*, and *Takagi*, and

*Bethards* to render obvious Appellant's invention of claim 6. Accordingly, the Board is respectfully requested to reverse the rejection of claim 6 under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Bethards*.

**Group 3, Claims 2-5 and 7-14, 16-17, and 19-20**

The Second Non-final Office Action rejected claims 3-4, and 8-9 under 35 U.S.C. 103(a) as being unpatentable over *Iijima* in view of *Takagi*. In addition, claim 2 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Tuttle*. Claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Tallman*. Claim 7 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Strohbeck*. Claim 10 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Weber*. Claim 11 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and *Weber* and further in view of *Flanagan*. Claim 12 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*, *Weber*, and *Flanagan*, and further in view of *Hansen*. Claim 13 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*, *Weber*, and *Flanagan*, and further in view of *Dodd*. Claim 14 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Bryant*. Claim 16 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Tallman*. Claim 17 was

rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Strohbeck*. Claim 19 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi* and further in view of *Bryant*. Claim 20 was rejected under 35 U.S.C. §103(a) as being unpatentable over *Iijima* in view of *Takagi*, *Weber*, *Flanagan*, *Hansen*, *Dodd*, and *Bryant*.

In summary, claims 2-5 and 7-14, 16-17, and 19-20 were rejected as being unpatentable over a combination of *Iijima* in view of *Takagi*, with some of the claims being rejected further in view of one or more of the following references: *Tuttle*, *Tallman*, *Strohbeck*, *Weber*, *Flanagan*, *Hansen*, *Dodd*, and *Bryant*.

Claims 2-5 and 7-14 depend directly or indirectly from claim 1. Accordingly, the rejections of claims 2-5 and 7-14 under 35 U.S.C. §103 are improper for the reasons set forth above in connection with group 1, claim 1. Therefore, Appellant believes the rejections of claims 2-5 and 7-14 under 35 U.S.C. §103 to be overcome.

In addition, due to the great number of disparate references cited in connection with this case, it is Appellant's position that the above-identified application was used as a blueprint, with the hypothetical combination of the *Iijima* and *Takagi* device as the main structural diagram. The other prior art was looked at for the elements present in the claimed invention but missing from the hypothetical combination of the *Iijima* and *Takagi* device. That is, the claims were used as a guide to selectively pick and choose elements from the various references so as to arrive at the claimed invention. However, rejections

based on hindsight are improper. As stated in Ex parte Clapp, 227 USPQ 972, 973 (B.P.A.I. 1985):

In the instant application, the examiner has done little more than cite references to show that one or more elements or subcombinations thereof, when each is viewed in a vacuum, is known. The claimed invention, however, is clearly directed to a combination of elements. That is to say, appellant does not claim that he has invented one or more new elements but has presented claims to a new combination of elements. To support the conclusion that the claimed combination is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed combination or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

The Second, Non-final Office Action does not discuss any specific evidence of motivation to combine, but only makes conclusory statements. However, "Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617.

For example, regarding claim 11, the Second, Non-final Office Action points to the *Flanagan* reference as a teaching of Appellant's claimed override switch. The Office Action concludes that it would have been obvious to include an override switch to continuously enable the ignition system, as taught by *Flanagan*, in the theoretical combination of *Iijima*, *Takagi*, and *Weber*.

*Flanagan* discloses an override relay that may be used to bypass an electrical interlock. In an exemplary use, *Flanagan* teaches of an electrical interlock used to disable an ignition

system until the driver and all of his passengers have fastened their seatbelts. The override relay functions to bypass the electrical interlock in the event of a failure of the electrical interlock system.

Appellant does not dispute that override switches and relays are known. However, Appellant's invention of claim 11 is directed to a new combination of elements that includes an override switch combined with the elements related to a vehicle theft protection system. None of the prior art of record expressly or impliedly suggests the inclusion of an override switch within a vehicle theft protection system, as recited in claim 11. Moreover, *Flanagan* merely offers the broad assertion that the magnetic relay can be employed in other environments to override an interlock or perform other functions to which its operation is suited.

The Office Action offers the conclusion that it would be obvious to combine the *Flanagan* override relay with the theoretical combination of *Iijima*, *Takagi*, and *Weber* with "the motivation for doing so would allow the override switch enabling the ignition system running." There appears to be little line of reasoning in this statement for making the combination in an attempt to render obvious Appellant's invention of claim 11. Rather, it is only Appellant's disclosure that teaches that which Appellant claims. Consequently, Appellant believes that one skilled in the art would not have found the invention of claim 11 obvious without using the claim as a guide to selectively pick and choose elements and concepts from the prior art.



Regarding claim 12, which depends from claim 11, a similar argument can be made. Claim 12 was rejected in view of a combination of *Iijima*, *Takagi*, *Weber*, and *Flanagan*, and further in view of *Hansen*. *Hansen* teaches of a circuit control device combining the functions of a current sensor, a time delay circuit, an undervoltage sensor, and a lockout such that, once tripped, the device must be reset intentionally. The Office Action alleged that the first four references failed to explicitly disclose the claim 12 limitation of the override switch causes the latching relay to remain latch to continuously enable the ignition system only following actuation of the latching relay.

The Office Action then asserts that the *Hansen* reference is in the same field of endeavor of a relay circuit device. It should be noted herein, that the *Hansen* reference is not in the same field of endeavor as a vehicle theft protection system which is the focus of the above-identified application. Nevertheless, the Office Action concludes that it would be obvious to combine the teaching of *Hansen* with a combination of *Iijima*, *Takagi*, *Weber*, and *Flanagan*. Since none of the prior art expressly or impliedly suggests the inclusion of an override switch within a vehicle theft protection system, it follows that the prior art cannot suggest a further limitation, recited in claim 12, related to the override capability of Appellant's vehicle theft protection system.

However, the Office Action asserts that such a combination is obvious with "the motivation for doing so would allow the override switch to cause latching relay to be latched continuously enabling the ignition system running." Again,

there appears to be little line of reasoning in this broad conclusory statement for making the combination. Rather, it is only Appellant's disclosure that teaches, and provides motivation for, the combination of claim 12. Consequently, Appellant believes that one skilled in the art would not have found the invention of claim 12 obvious without using the claim as a guide to selectively pick and choose elements and concepts from the prior art.

Claim 13 also depends from claim 11. Claim 13 was rejected in view of a combination of *Iijima, Takagi, Weber, and Flanagan*, and further in view of *Dodd*. *Dodd* teaches of a vehicle wheel safety barrier system that prevents a person from being caught under the wheel of a vehicle. The safety barrier system is provided with a sensing system to inform the driver of the presence of the person on the barrier during startup. The safety barrier system includes a manual override switch to allow the vehicle driver to turn the system off. While the system is off a warning light will remain on.

Again, Appellant does not dispute that it is known to include indicators to indicate when a switch is activated. However, Appellant's invention of claim 13 is directed to a new combination of elements that includes an override switch and an override indicator combined with the elements related to a vehicle theft protection system. None of the prior art of record expressly or impliedly suggests the inclusion of an override switch within a vehicle theft protection system. . Therefore, it follows that the prior art cannot suggest a further limitation, recited in claim 13, related to the override capability of Appellant's vehicle theft protection system.

Consequently, Appellant believes that one skilled in the art would not have found the invention of claim 13 obvious without using the claim as a guide to selectively pick and choose elements and concepts from the prior art.

Yet the same situation arises with regard to claim 14. Claim 14 was rejected in view of a combination of *Iijima* and *Takagi* and further in view of *Bryant*. *Bryant* teaches of a vehicle antenna system to transfer energy between a radio transceiver (i.e., a cellular telephone) located inside a vehicle and an external radiator mounted on the outside of the vehicle. The *Bryant* vehicle antenna system functions as a wireless repeater system to gain the benefit of a vehicle-mounted antenna without making or breaking wired connections each time the cellular telephone is moved.

The Office Action asserts that *Bryant* is in the same field of endeavor of vehicle antenna systems. Again it should be noted that the *Bryant* reference is not, however, in the same field of endeavor as a vehicle theft protection system which is the focus of the above-identified application. Rather, *Bryant* is related to the field of cellular telephony.

Furthermore, the alleged motivation for combining the teaching of *Bryant* with *Iijima* and *Takagi* is to "allow the communication of an on board controller with the transponder." Of course, one might argue that the motivation of any antenna system is to allow communication between two antenna elements. But, this line of reasoning is not clear as to how or why one would place an antenna of a vehicle theft prevention system inside a passenger compartment as claimed. *Iijima* teaches the

use of the vehicular antenna (col. 4, lines 22-33) in communication with the transponder in the key, and alternatively, an antenna unit arranged in the ignition key cylinder of the motor vehicle (col. 7, lines 31-32). *Takagi* teaches the use of an antenna 22 (col.2, lines 39-41), but provides no teaching of its location.

In contrast, Appellant teaches that the antenna may be embedded inside or beneath the driver side seat cushion within the passenger compartment so that the antenna and the transponder (which is separate from the key) are likely to be in close proximity, for example, within twenty inches, in order for the interrogator circuit to detect the return signal (page 8, line 25, through page 9, line2). Accordingly, only Applicant teaches that which is being claimed.

For the reasons set forth above, disparate references were improperly combined in an attempt to deprecate Appellant's invention of claim 14. Moreover, no convincing line of reasoning as to why the claimed invention is obvious in light of the teachings of the references has been presented in connection with claim 14. Thus, Appellant believes that one skilled in the art would not have found the invention of claim 14 obvious without using the claim as a guide to selectively pick and choose elements and concepts from the prior art.

Claims 16-17 depend from claim 15. Consequently, the rejection of claims 16-17 is also improper for the reasons set forth above in connection with group 1, claim 1. In addition, claim 16 is allowable for the reasons set forth in connection with group 2, claim 6. Claims 19-20 depend from independent

claim 18. Consequently, the rejection of claims 19-20 is also improper for the reasons set forth above in connection with group 1, claim 1. In addition, claim 19 is allowable for the reasons set forth in connection with group 3, claim 14, and claim 20 is allowable for the reasons set forth in connection with group 3, claim 11, 12, and 13.

Evidence presented herein indicates that hindsight has been used in making a host of obviousness rejections based on disparate references. In particular, the claims were used as a guide to selectively pick and choose elements from the various references so as to arrive at the claimed invention. However, rejections based on hindsight are improper. Accordingly, the Board is respectfully requested to reverse the rejections of claims 2-5, 7-14, 16-17, and 19-20 under 35 U.S.C. §103(a).

#### Conclusion

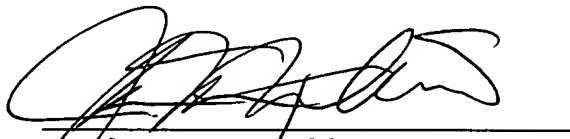
Claims 1-20 are included in this appeal.

The rejection of claims 1, 3-4, 8-9, 15 and 18 under 35 U.S.C. 103(a) as being unpatentable over *Iijima* in view of *Takagi* is believed improper. Likewise, the rejection of claim 2 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima*, and *Tuttle* is believed improper. The rejection of claim 5 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima*, *Takagi*, and *Tallman* is believed improper. The rejection of 6 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima*, *Takagi*, and *Bethards* is believed improper. The rejection of claim 7 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima*, *Takagi*, and *Strohbeck* is believed improper. The rejection of claim 10 under 35 U.S.C. §103(a) as being unpatentable over a combination of

*Iijima, Takagi, Weber* is believed improper. The rejection of claim 11 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi, Weber*, and *Flanagan* is believed improper. The rejection of claim 12 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi, Weber, Flanagan*, and *Hansen*. The rejection of claim 13 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi, Weber, Flanagan*, and *Dodd* is believed improper. The rejection of claim 14 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi*, and *Bryant*. The rejection of claim 16 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi*, and *Tallman* is believed improper. The rejection of claim 17 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi*, and *Strohbeck* is believed improper. The rejection of claim 19 under 35 U.S.C. §103(a) as being unpatentable over *Iijima, Takagi*, and *Bryant*, and the rejection of claim 20 under 35 U.S.C. §103(a) as being unpatentable over a combination of *Iijima, Takagi, Weber, Flanagan, Hansen, Dodd*, and *Bryant* is believed improper. In general, the references are silent as to any articulated or implied motivation for the modifications suggested in the Second, Non-final Office Action. In addition, the references are based on hindsight in which the claims are used as a guide to selectively pick and choose elements from the various references so as to arrive at the claimed invention. However, lack of a suggestion for combination and hindsight are improper standards for holding claims to be unpatentable.

Appellant believes that the arguments above fully respond to every outstanding ground of rejection and that the contested claims should be found allowable.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'J. Meschkow', is written over a horizontal line.

Jordan M. Meschkow  
Attorney for Applicant  
Reg. No. 31,043

Dated: 16 August 2004

Jordan M. Meschkow  
Meschkow & Gresham, P.L.C.  
5727 North Seventh Street  
Suite 409  
Phoenix, AZ 85014  
(602) 274-6996

## **(9) APPENDIX I -- Claims On Appeal**

1. An automatic vehicle theft prevention system for selectively enabling an ignition system of a vehicle, said ignition system being operable using an ignition key, and said system comprising:

an interrogator circuit including a signal generator for generating an excitation signal and an antenna coupled to said signal generator for radiating said excitation signal and receiving a return signal;

a transponder circuit separate from said ignition key for detecting said excitation signal and radiating said return signal, said transponder circuit modulating said excitation signal to produce said return signal containing an identification code for said transponder circuit;

a controller in communication with said antenna for detecting said identification code in said return signal; and

a relay actuated to an enable mode by said controller when said controller detects said identification code, said relay being actuated to enable said ignition system.



2. A system as claimed in claim 1 wherein said transponder circuit is a mobile radio frequency identification (RFID) data carrier including a memory element for storing said identification code.

3. A system as claimed in claim 1 wherein said excitation signal provides power to said transponder circuit.

4. A system as claimed in claim 1 wherein said controller comprises:

an input for receiving a predetermined authorized identification code; and

a memory element in communication with said input for storing said predetermined authorized identification code, said controller actuating said relay to said enable mode in response to a match between said detected identification code and said predetermined authorized.

5. A system as claimed in claim 4 wherein said input is a data port configured for interconnection with an external programming device, said external programming device providing said predetermined authorized access code.

6. A system as claimed in claim 4 wherein said input is said antenna configured for radio frequency communication with an external programming device, said external programming device providing said predetermined authorized access code.

7. A system as claimed in claim 4 wherein:  
said identification code is a first identification code;  
said predetermined authorized identification code is a first predetermined authorized identification code;

said input of said controller is configured to receive a second predetermined authorized identification code;

said memory element is configured to store said second predetermined authorized identification code; and

said system further comprises a second RFID data carrier separate from said ignition key for detecting said excitation signal and radiating said return signal, said second RFID data carrier including a memory element for storing a second identification code for said second RFID data carrier, and said second RFID data carrier modulating said excitation signal to produce said return signal containing said second identification code, wherein when said controller detects a match between said detected second identification code and said second predetermined authorized identification code, said relay is actuated to said enable mode to enable said ignition system.

8. A system as claimed in claim 1 wherein said relay is actuated to a disable mode whenever said controller fails to detect said identification code.

9. A system as claimed in claim 1 wherein said ignition system includes an ignition switch and a starter mechanism, and said system further comprises:

an input configured to be coupled to an output of said ignition switch, and said input being in communication with an input of said relay; and

an output in communication with an enable mode output of said relay and configured to be coupled to an input of said starter mechanism.

10. A system as claimed in claim 1 wherein said ignition system includes an ignition switch activated by said ignition key, and said system further includes a latching relay actuated in response to a momentary actuation of said relay when said controller detects said identification code, said latching relay being adapted to remain latched until said ignition switch is deactivated.

11. A system as claimed in claim 10 further comprising an override switch in communication with an input of said latching relay wherein activation of said override switch causes said latching relay to be latched to continuously enable said ignition system.

12. A system as claimed in claim 11 wherein activation of said override switch causes said latching relay to remain latched to continuously enable said ignition system only following actuation of said latching relay by said relay.

13. A system as claimed in claim 11 further comprising an indicator in communication with an output of said override switch and energized when said override switch is activated.

14. A system as claimed in claim 1 wherein said antenna is configured for placement inside a passenger compartment of said vehicle.

15. An automatic vehicle theft prevention system for selectively enabling an ignition system of a vehicle, said ignition system being operable using an ignition key, and said system comprising:

an interrogator circuit including a signal generator for generating an excitation signal and an antenna coupled to said signal generator for radiating said excitation signal and receiving a return signal;

a mobile radio frequency identification (RFID) data carrier separate from said ignition key for detecting said excitation signal and radiating said return signal, said RFID data carrier including a memory element for storing an identification code for said RFID data carrier, and said RFID data carrier modulating said excitation signal to produce said return signal containing said identification code;

a controller in communication with said antenna for detecting said identification code in said return signal, said controller including:

an input for receiving a predetermined authorized identification code; and

a memory element in communication with said input for storing said predetermined authorized identification code; and

a relay actuated to an enable mode by said controller when said controller detects a match between said detected identification code and said predetermined authorized identification code, said relay being actuated to said enable mode to enable said ignition system.

16. A system as claimed in claim 15 wherein said input is one of a data port and said antenna, said data port being configured for interconnection with an external programming device, and said antenna being configured for radio frequency communication with said external programming device, said external programming device providing said predetermined authorized access code.

17. A system as claimed in claim 15 wherein:  
said identification code is a first identification code;  
said predetermined authorized identification code is a first predetermined authorized identification code;

said input of said controller is configured to receive a second predetermined authorized identification code;

said memory element is configured to store said second predetermined authorized identification code; and

said system further comprises a second RFID data carrier separate from said ignition key for detecting said excitation signal and radiating said return signal, said second RFID data

carrier including a memory element for storing a second identification code for said second RFID data carrier, and said second RFID data carrier modulating said excitation signal to produce said return signal containing said second identification code, wherein when said controller detects a match between said detected second identification code and said second predetermined authorized identification code, said relay is actuated to said enable mode to enable said ignition system.

18. An automatic vehicle theft prevention system for selectively enabling an ignition system of a vehicle, said ignition system being operable using an ignition key, and said system comprising:

an interrogator circuit including a signal generator for generating an excitation signal and an antenna coupled to said signal generator for radiating said excitation signal and receiving a return signal;

a mobile radio frequency identification (RFID) data carrier separate from said ignition key for detecting said excitation signal and radiating said return signal, said mobile RFID data carrier including a memory element for storing an identification code for said mobile RFID data carrier, said mobile RFID data

carrier modulating said excitation signal to produce said return signal containing said identification code;

a controller in communication with said antenna for detecting said identification code in said return signal; and

a relay actuated by said controller to one of an enable mode and a disable mode, said relay being actuated to said enable mode to enable said ignition system in response to detection of said identification code, and said relay being actuated to said disable mode to disable said ignition system whenever said controller fails to detect said identification code.

19. A system as claimed in claim 18 wherein said antenna is configured for placement inside a passenger compartment of said vehicle.



20. A system as claimed in claim 19 further comprising:

a latching relay actuated in response to a momentary actuation of said relay when said controller detects said identification code, said latching relay being adapted to remain latched until said ignition switch is deactivated;

an override switch in communication with an input of said latching relay wherein activation of said override switch causes said latching relay to remain latched to continuously enable said ignition system only following actuation of said latching relay by said relay; and

an indicator in communication an output of said override switch and energized when said override switch is activated.

## **APPENDIX II**



US005708307A

**United States Patent** [19]

Iijima et al.

[11] Patent Number: **5,708,307**[45] Date of Patent: **Jan. 13, 1998**[54] **ANTI-THEFT CAR PROTECTION SYSTEM**

[75] Inventors: **Yohichi Iijima, Hadano; Yoshiki Onuma, Ebina; Takashi Yoshizawa, Atsugi, all of Japan**

[73] Assignee: **Nissan Motor Co., Ltd., Kanagawa, Japan**

[21] Appl No.: **546,800**

[22] Filed: **Oct. 23, 1995**

[30] **Foreign Application Priority Data**

Nov. 2, 1994	[JP]	Japan	6-269394
Dec. 7, 1994	[JP]	Japan	6-303518
Dec. 7, 1994	[JP]	Japan	6-303519
Dec. 9, 1994	[JP]	Japan	6-306290

[51] Int. Cl.<sup>6</sup> **B60R 25/10**

[52] U.S. Cl. **307/10.5; 307/10.3; 307/10.4; 307/10.5; 307/10.2; 180/287; 340/426**

[58] Field of Search **307/9.1-10.8; 364/424.01-424.05; 180/287, 167; 361/171, 172; 340/825.31, 825.34, 825.69, 825.72, 825.32, 426, 425.5; 123/198 B, 198 DB, 198 DC**

[56] **References Cited****U.S. PATENT DOCUMENTS**

4,236,594	12/1980	Ramsperger	180/167
4,965,460	10/1990	Tanaka et al.	307/10.4
5,519,260	5/1996	Washington	307/10.5
5,519,376	5/1996	Iijima	307/10.3

5,528,086	6/1996	Maass	307/10.5
5,539,260	7/1996	Khangura	307/10.3
5,554,891	9/1996	Shimizu	307/10.3
5,583,383	12/1996	Denz	307/10.5

**FOREIGN PATENT DOCUMENTS**

44 12 214	10/1994	Germany	
44 22 296	11/1994	Germany	
61-122379	6/1986	Japan	
64-56248	3/1989	Japan	
64-56253	3/1989	Japan	
2 269 253	2/1994	United Kingdom	
2 285 160	6/1995	United Kingdom	
2289357	11/1995	United Kingdom	307/10.5

**OTHER PUBLICATIONS**

The Present State and Trends of the Vehicle Burglar-Proof Systems—Car and Technology, vol. 48, Nov. 8, 1994, pp. 56-64.

Primary Examiner—William M. Shoop, Jr.

Assistant Examiner—Peter Ganjian

Attorney, Agent, or Firm—Lowe, Price, LeBlanc & Becker

## [57]

**ABSTRACT**

An anti-theft car protection system comprises a transmitter-receiver for receiving a code of the key, an immobilizer unit for collating said code as received with a code as registered and transmitting an engine start permission signal to an engine control unit when said code as received coincides with said code as registered, and means, cooperating with said immobilizer unit, for removing repetition of key operation upon start of the engine.

50 Claims, 20 Drawing Sheets

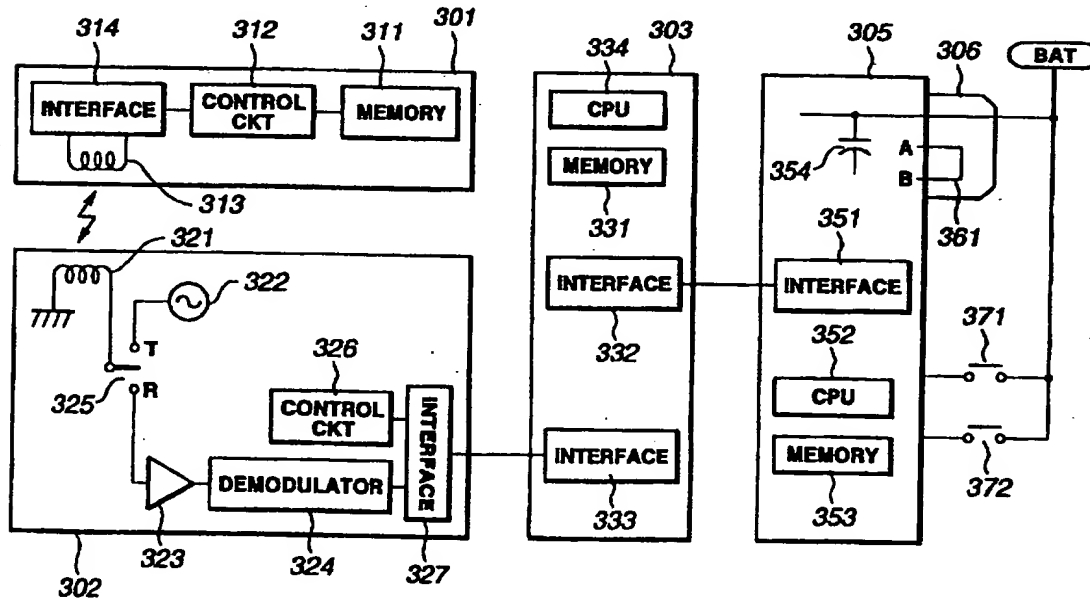


FIG. 1

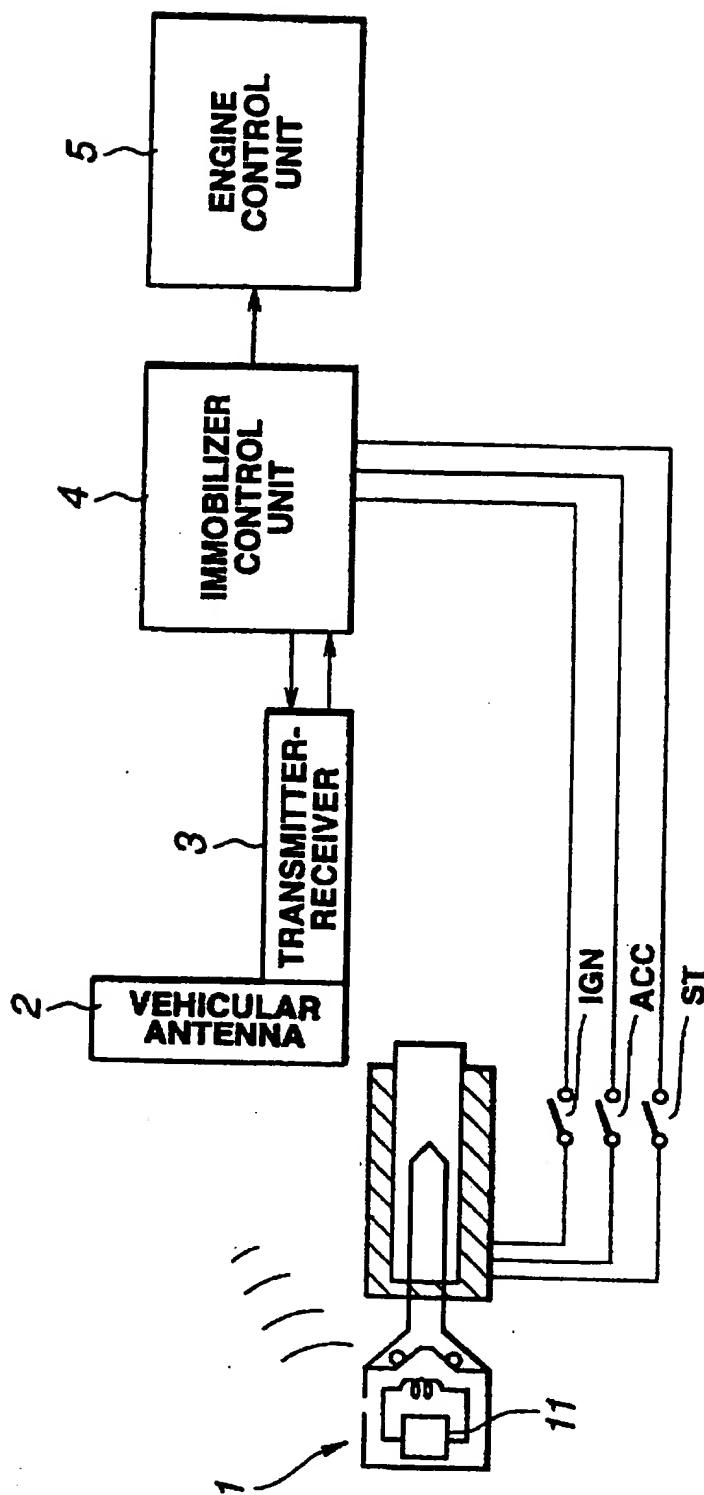


FIG.2A

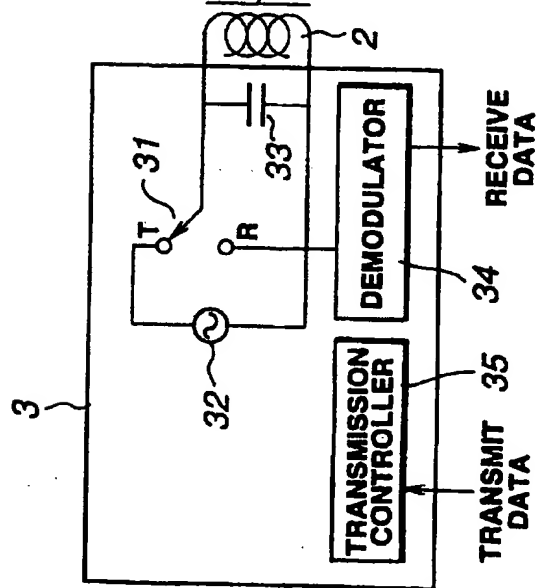


FIG.2B

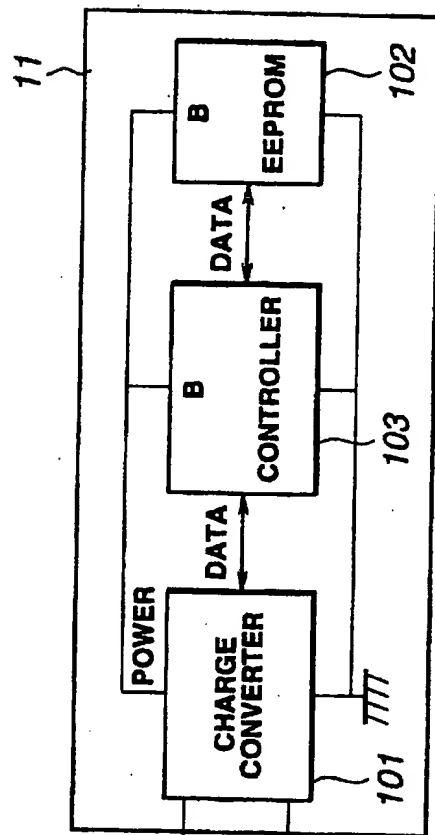


FIG. 3

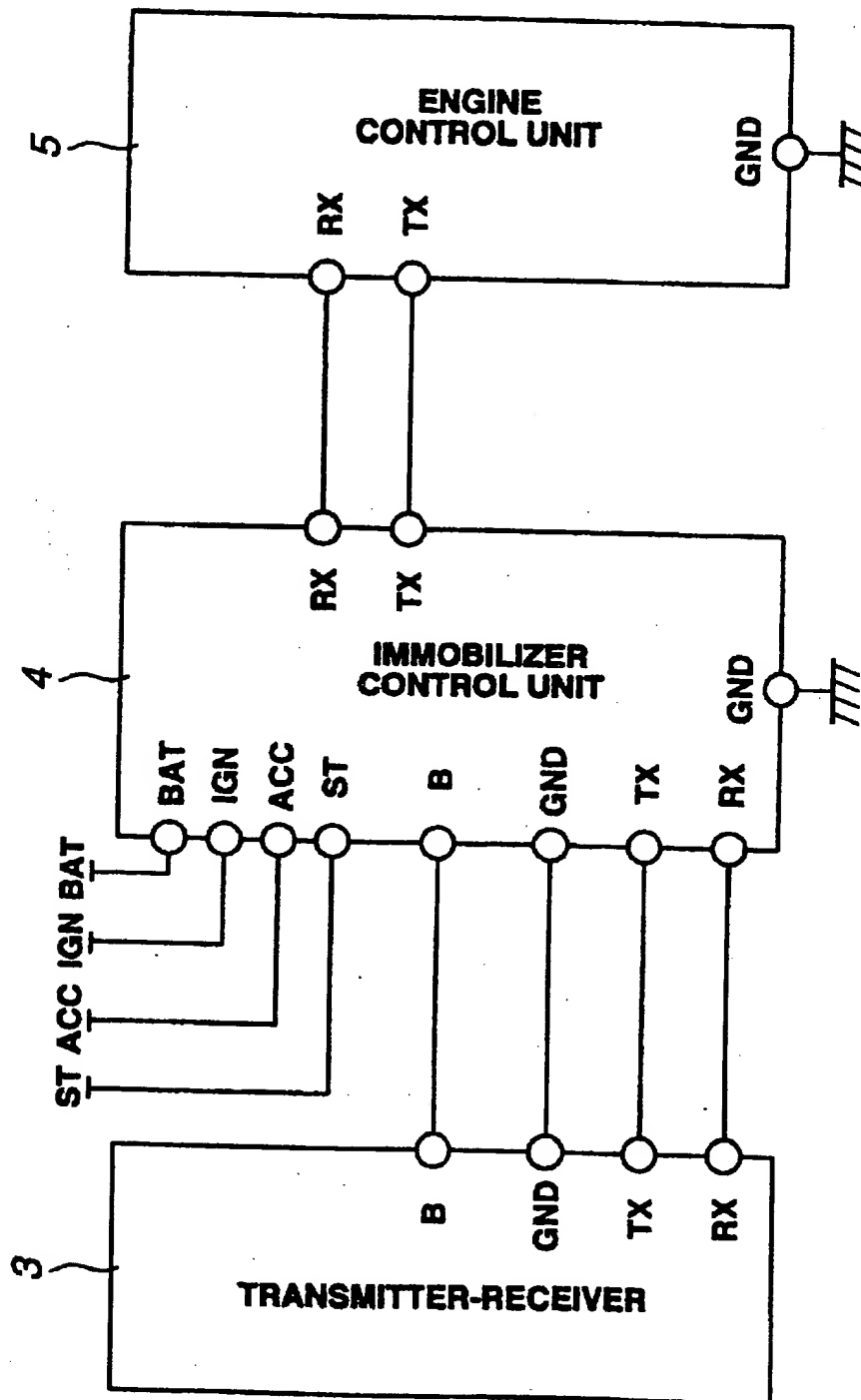


FIG. 4

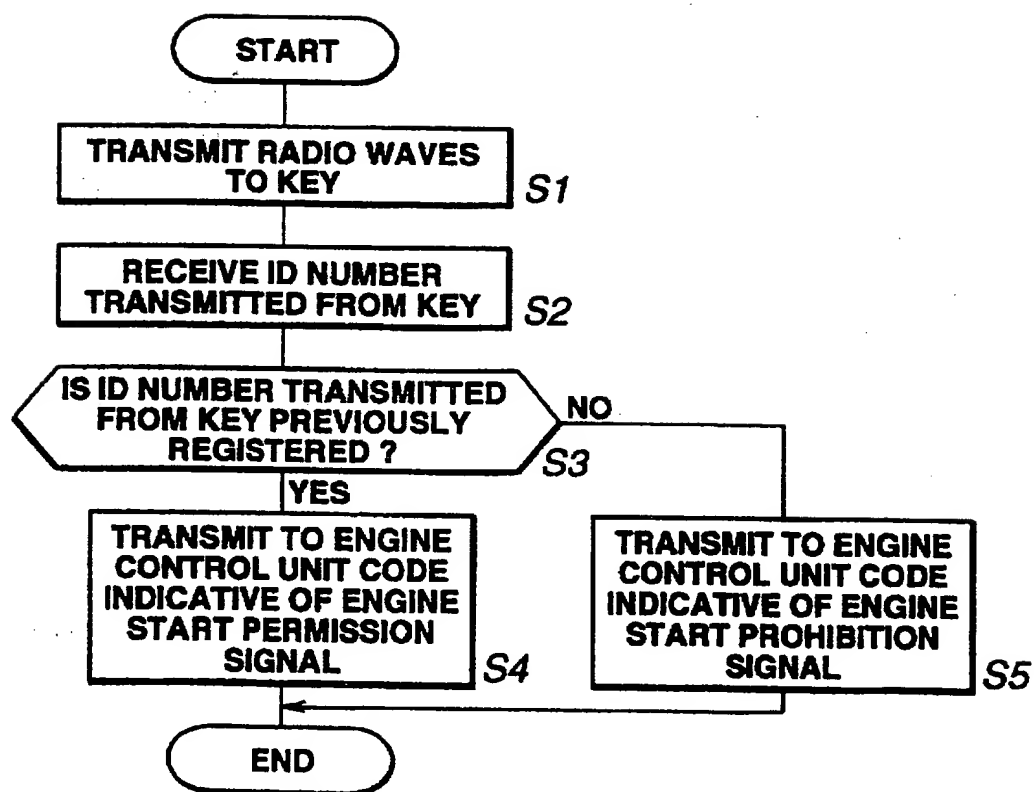


FIG. 5

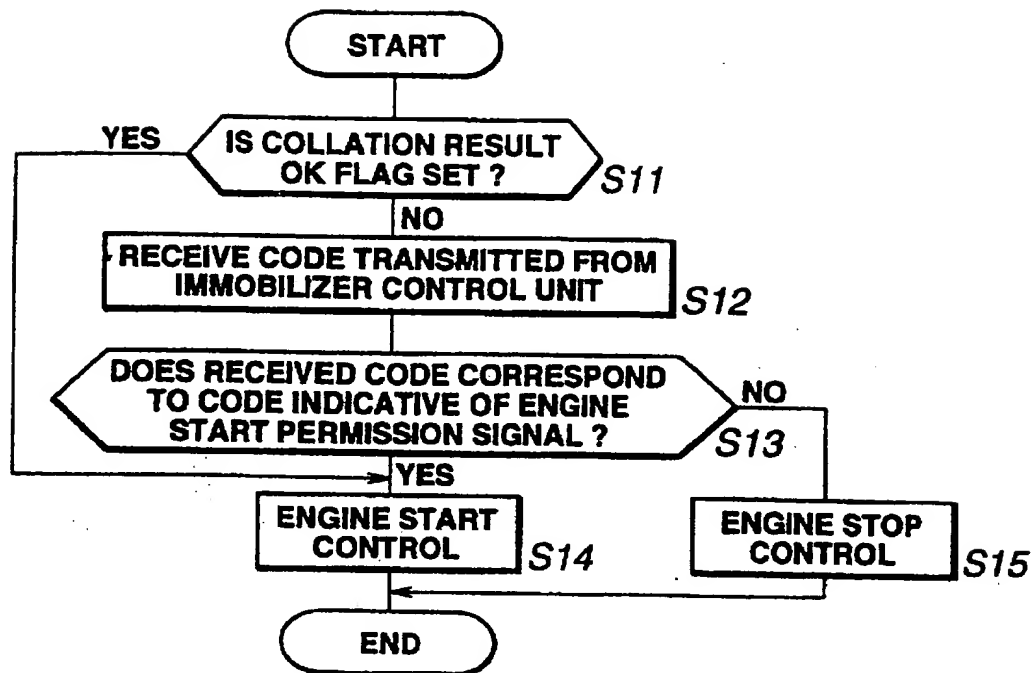


FIG. 6

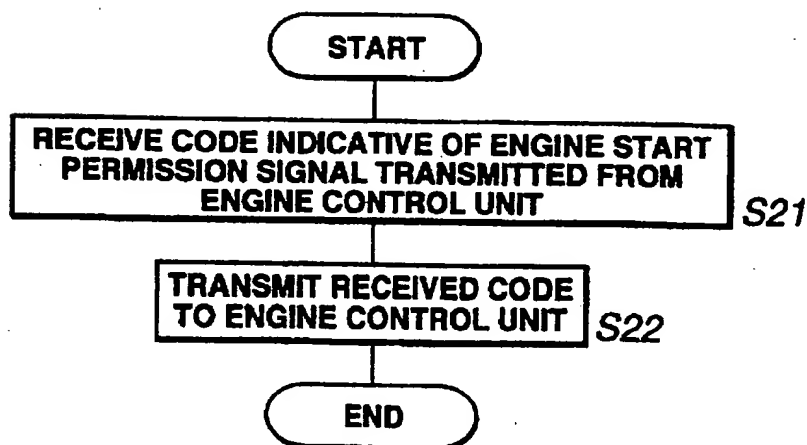




FIG. 7

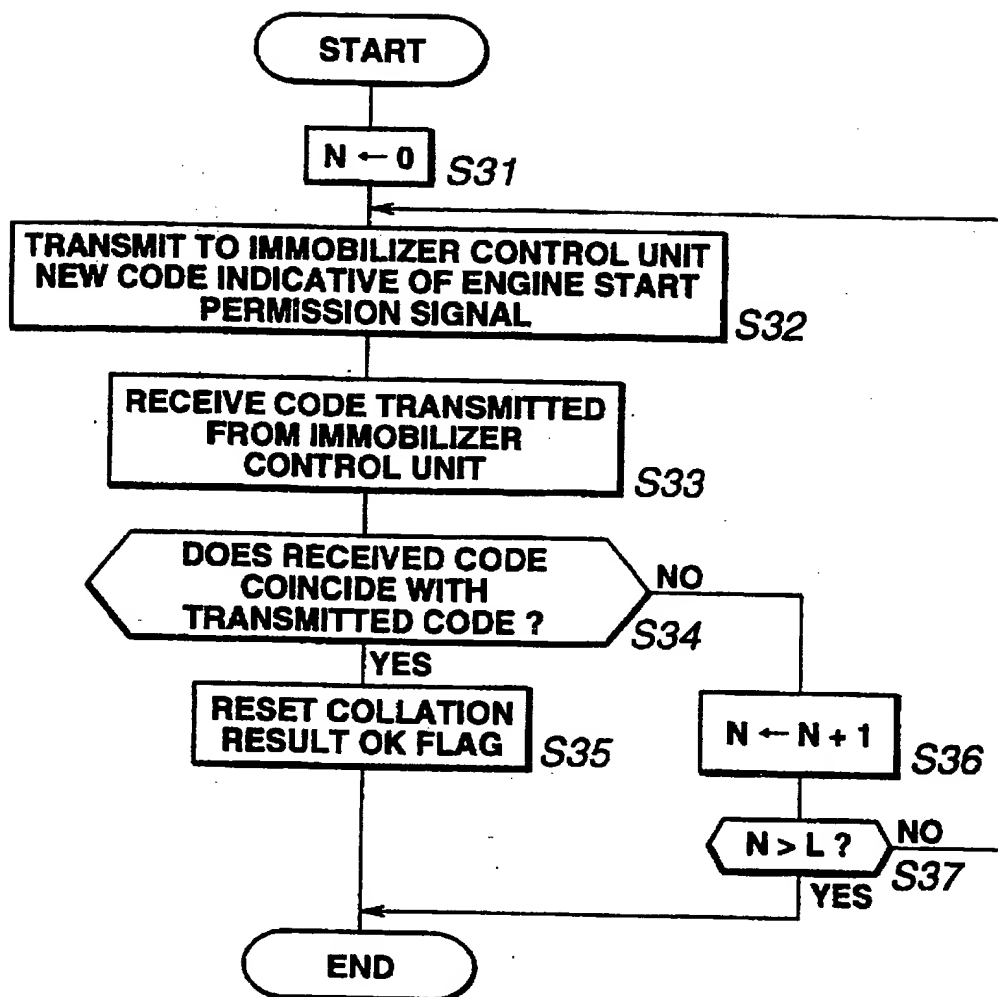


FIG. 8

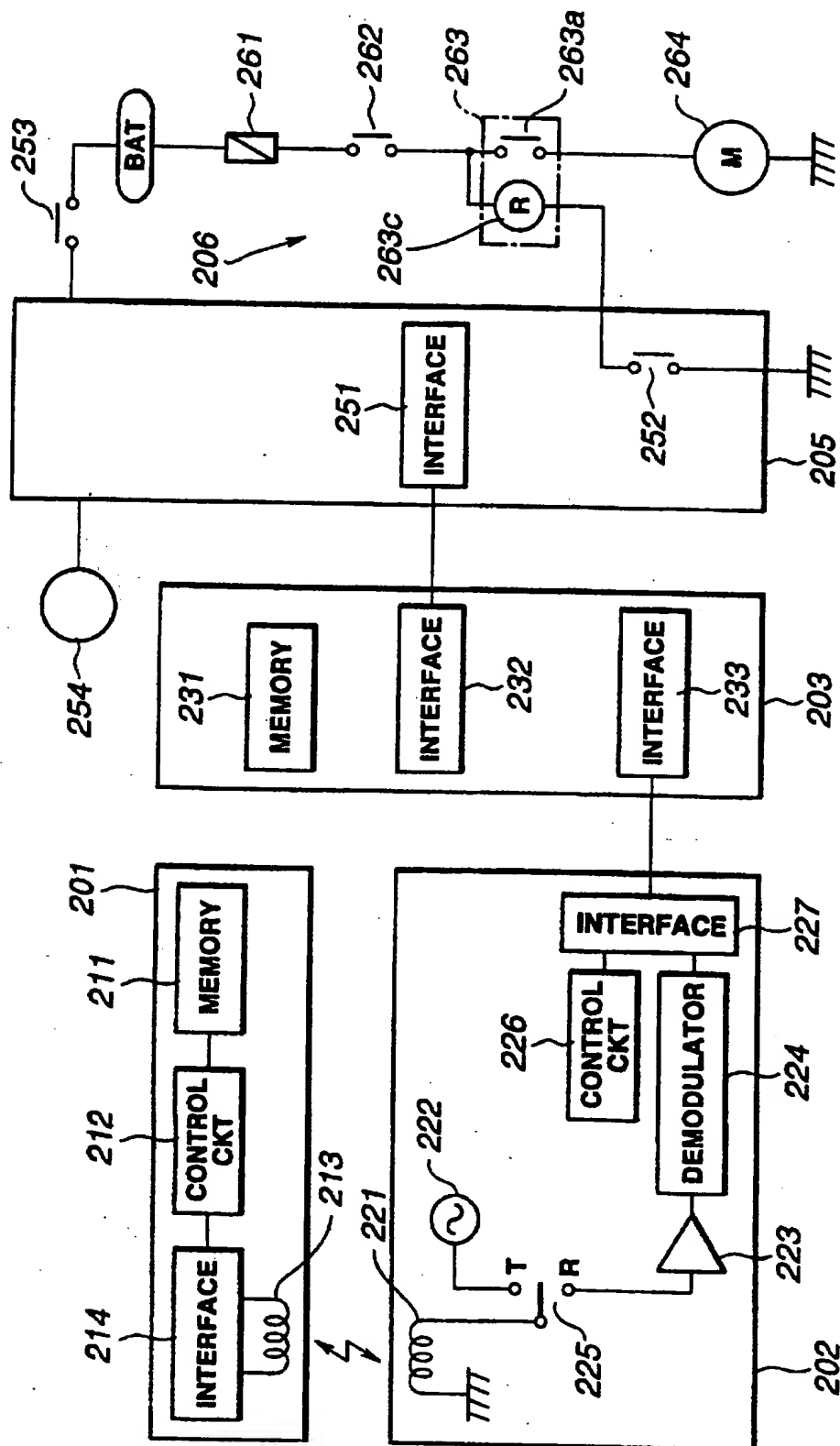


FIG. 9

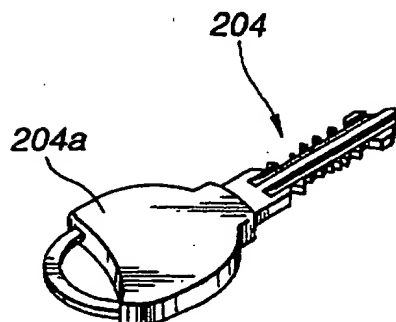


FIG. 10

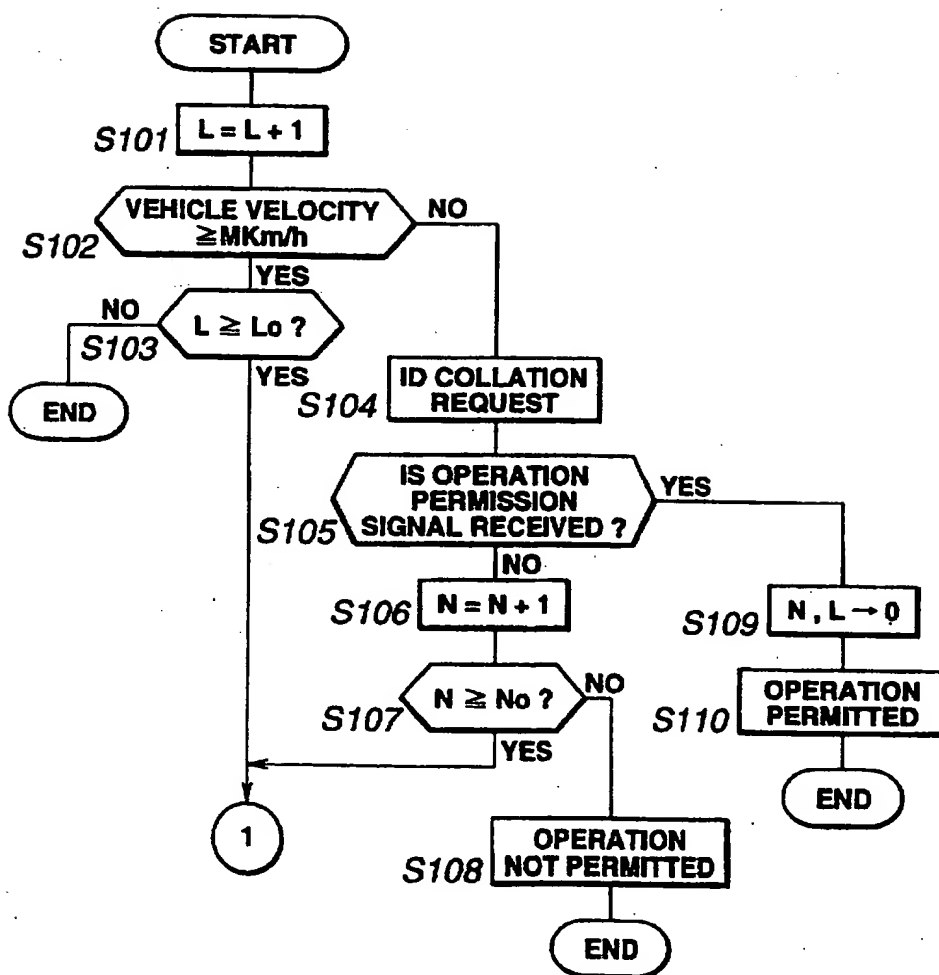


FIG. 11

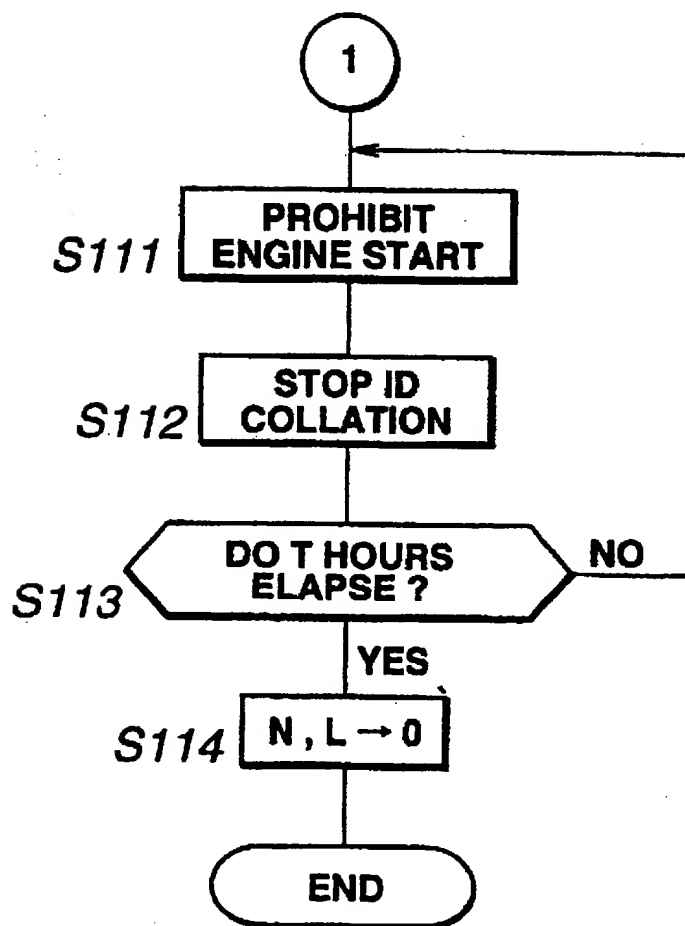


FIG. 12

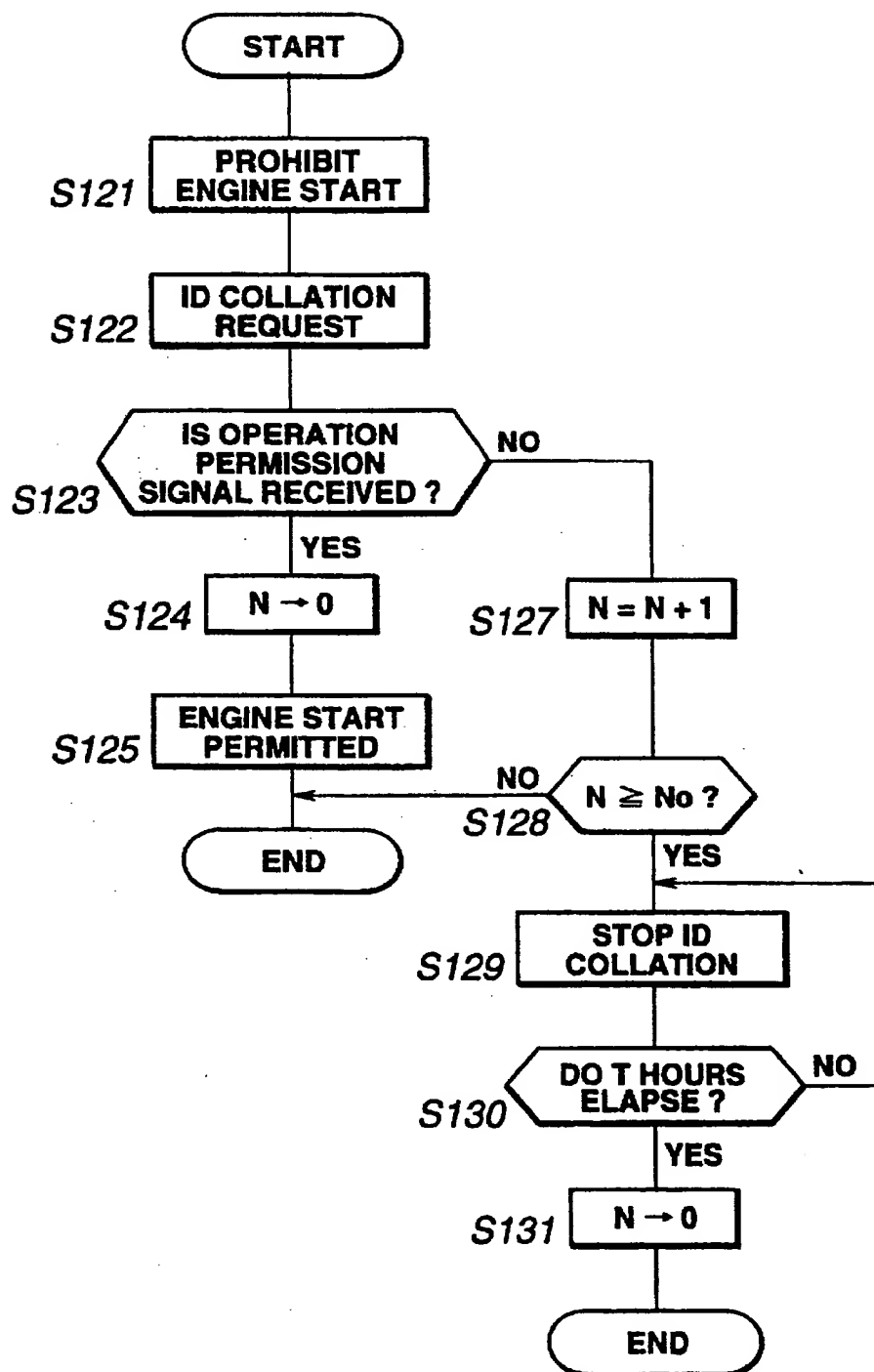


FIG. 13

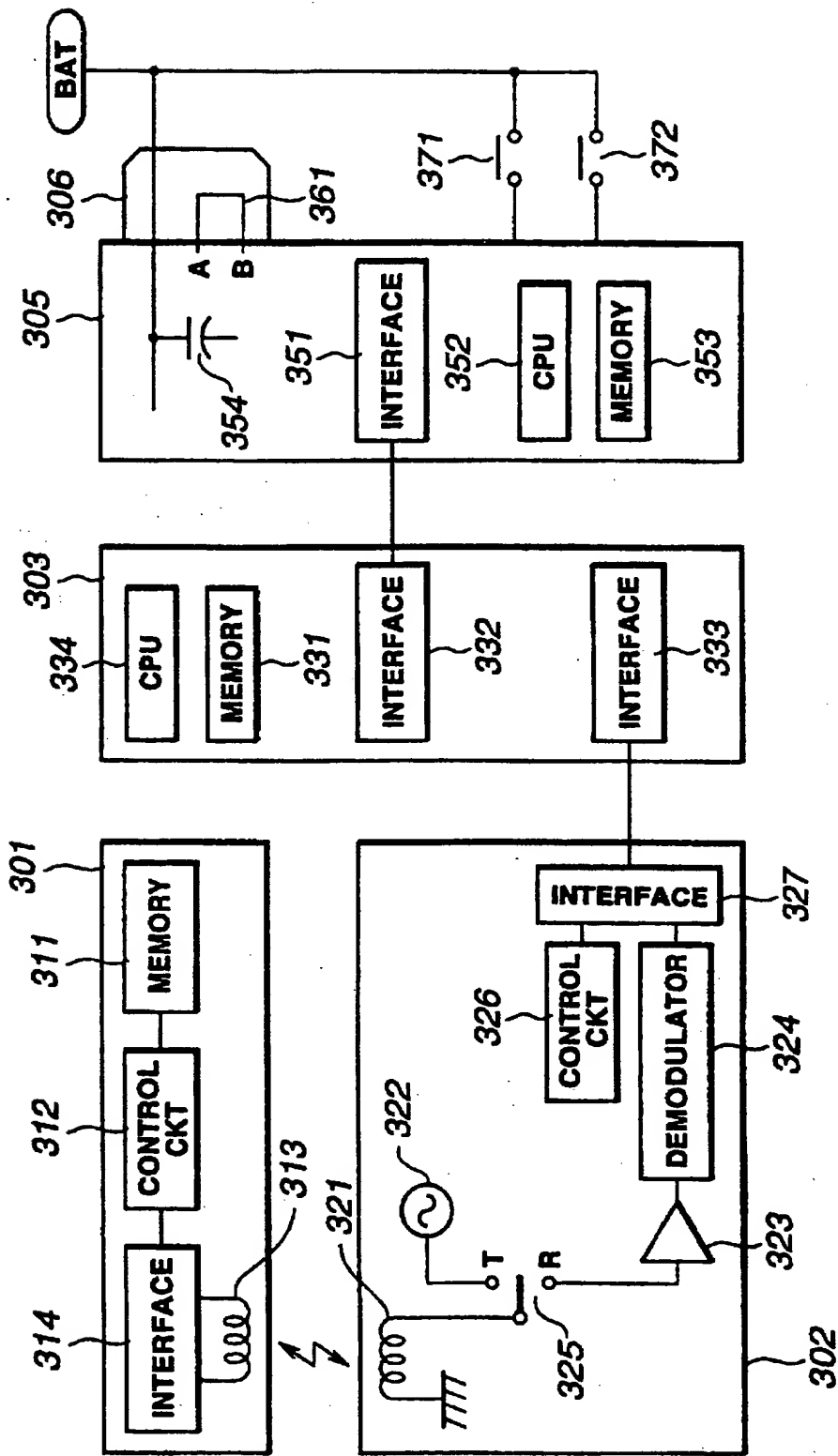


FIG. 14

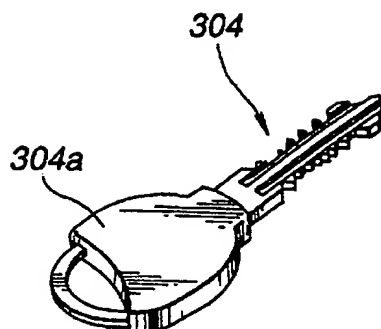


FIG. 15

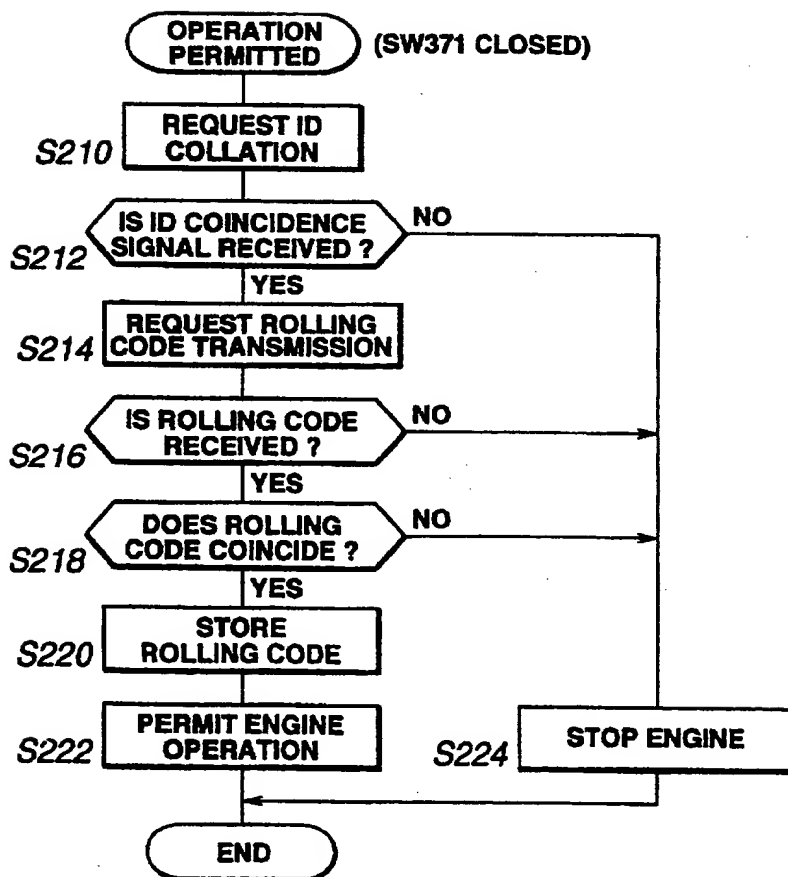


FIG. 16

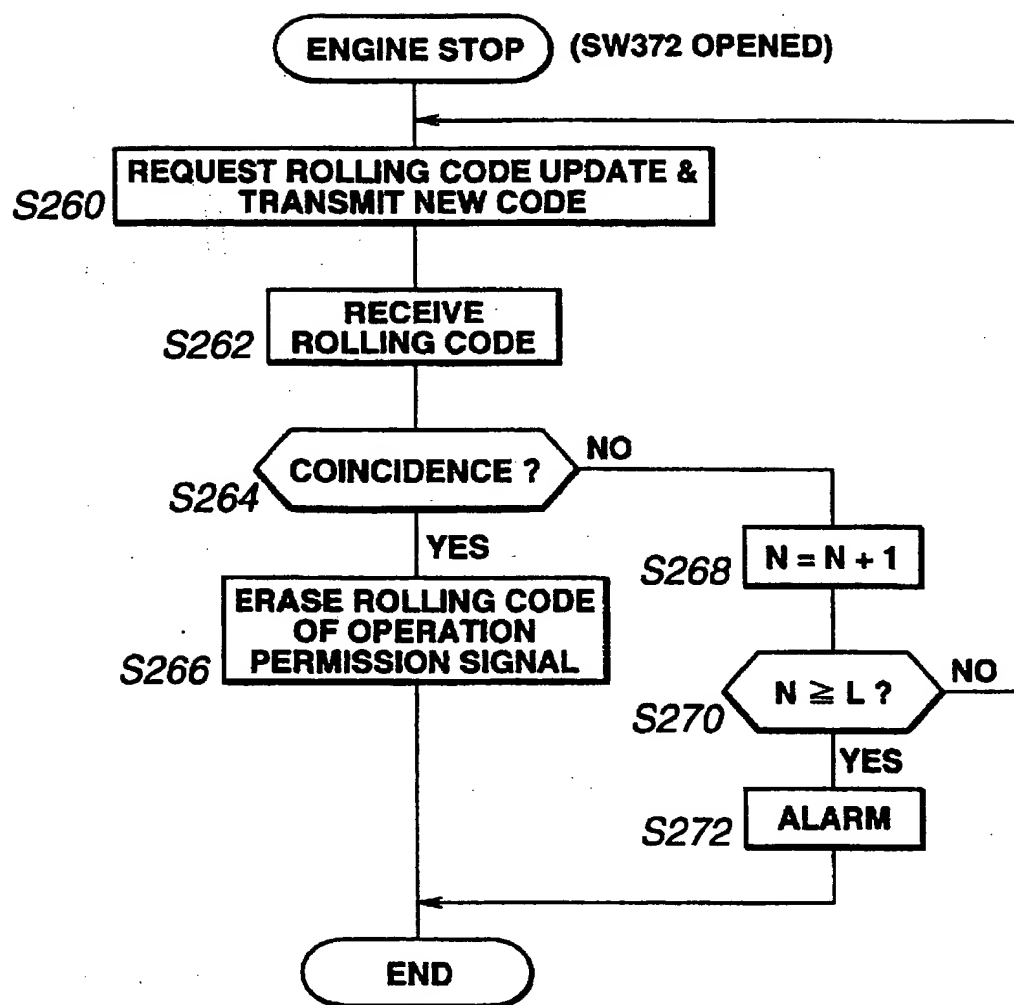
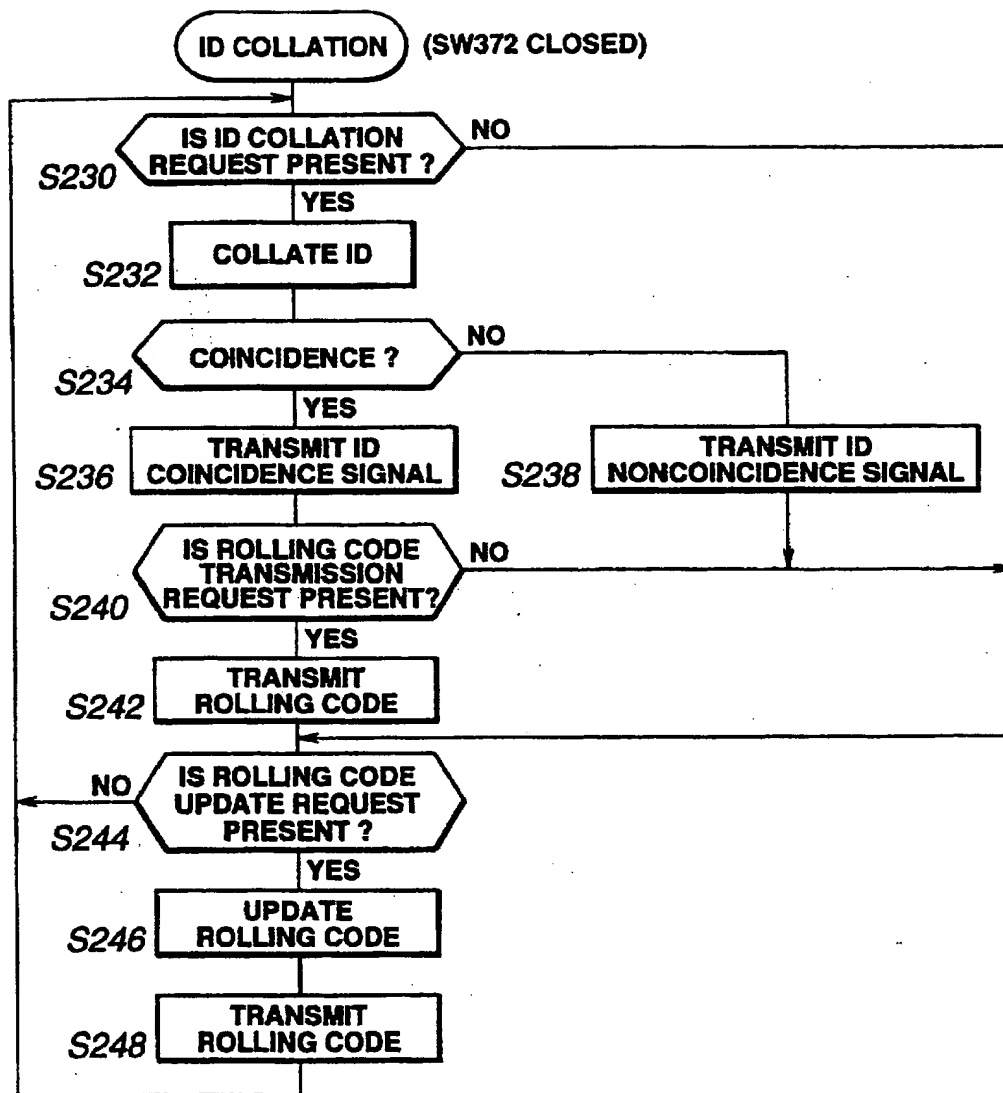




FIG.17



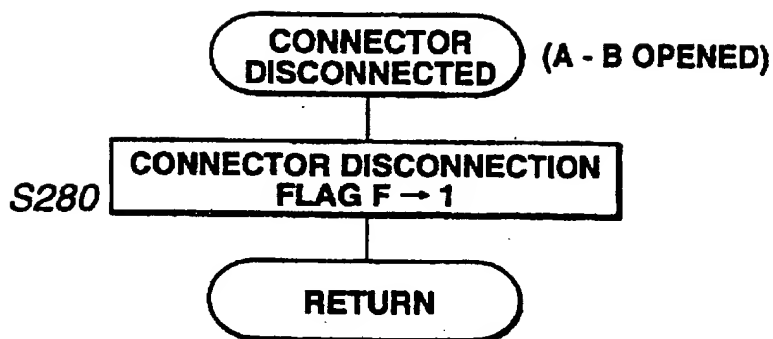
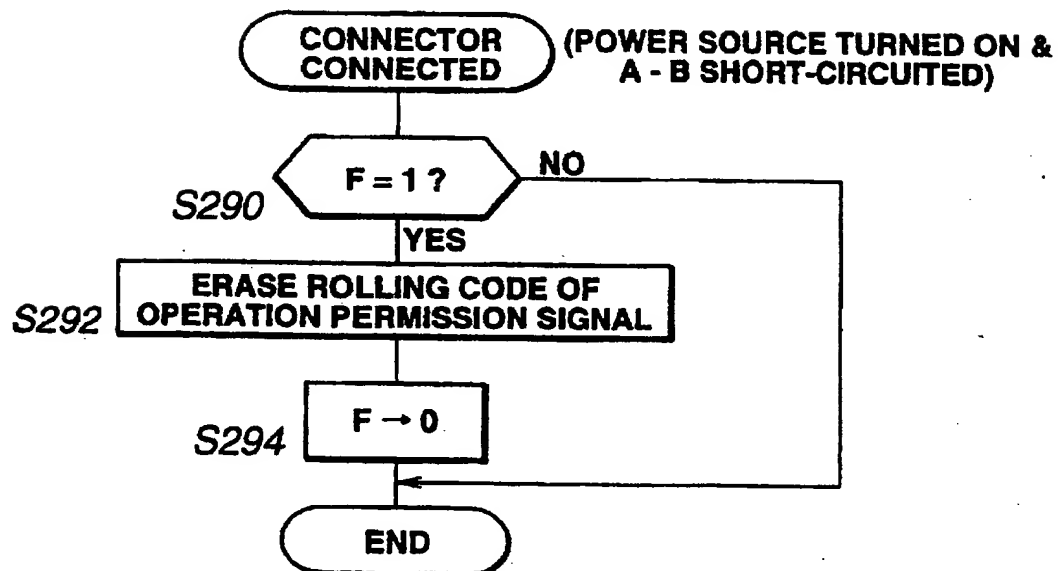
**FIG.18****FIG.19**



FIG. 21

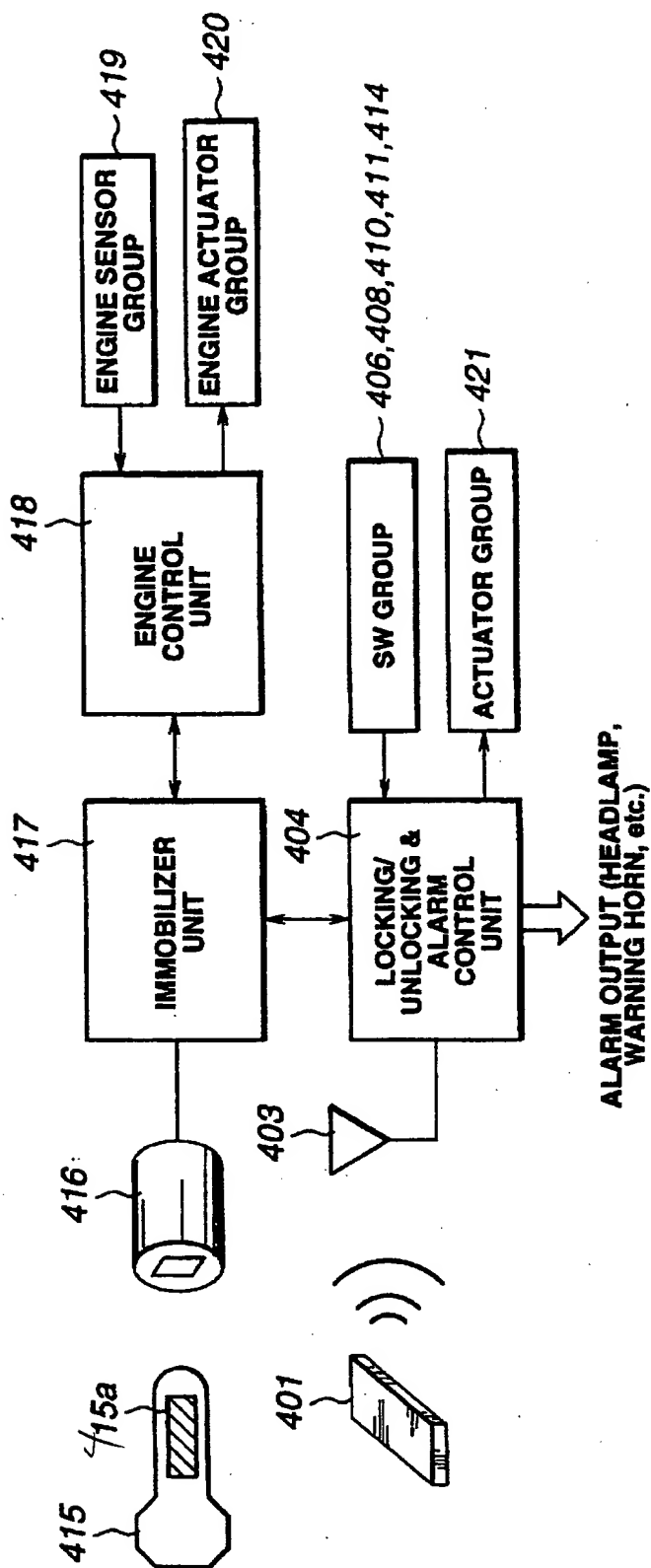


FIG.22

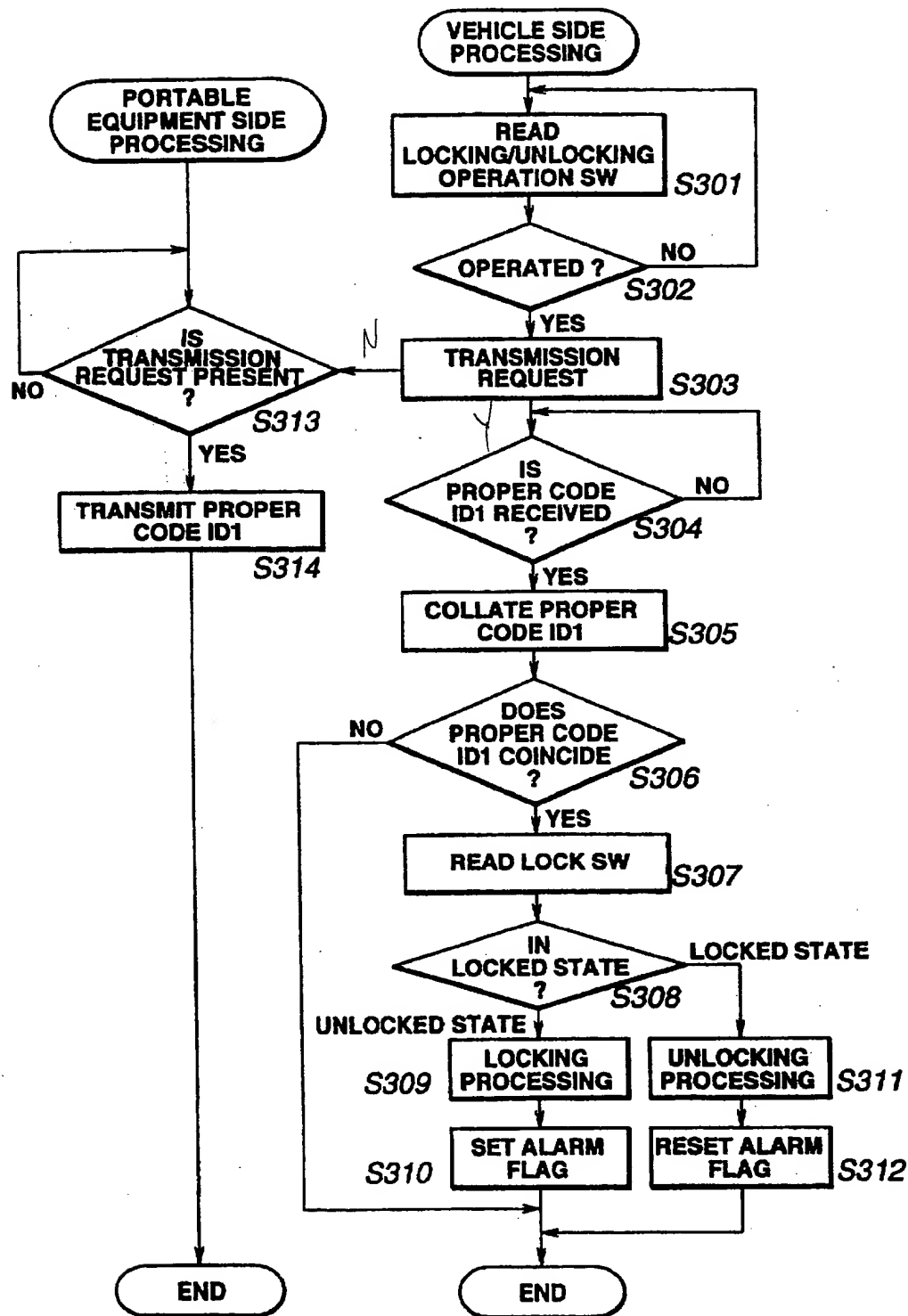


FIG. 23

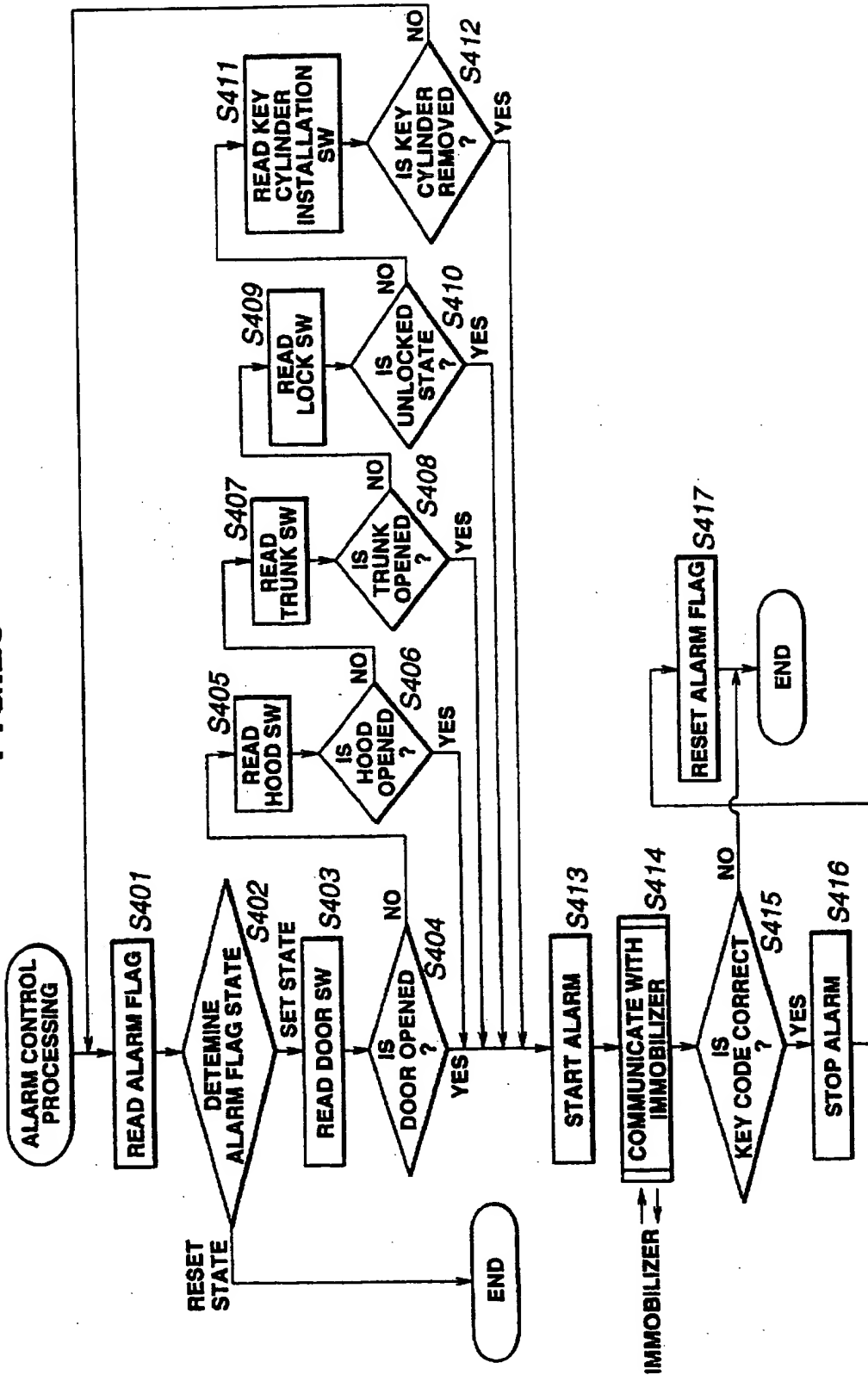
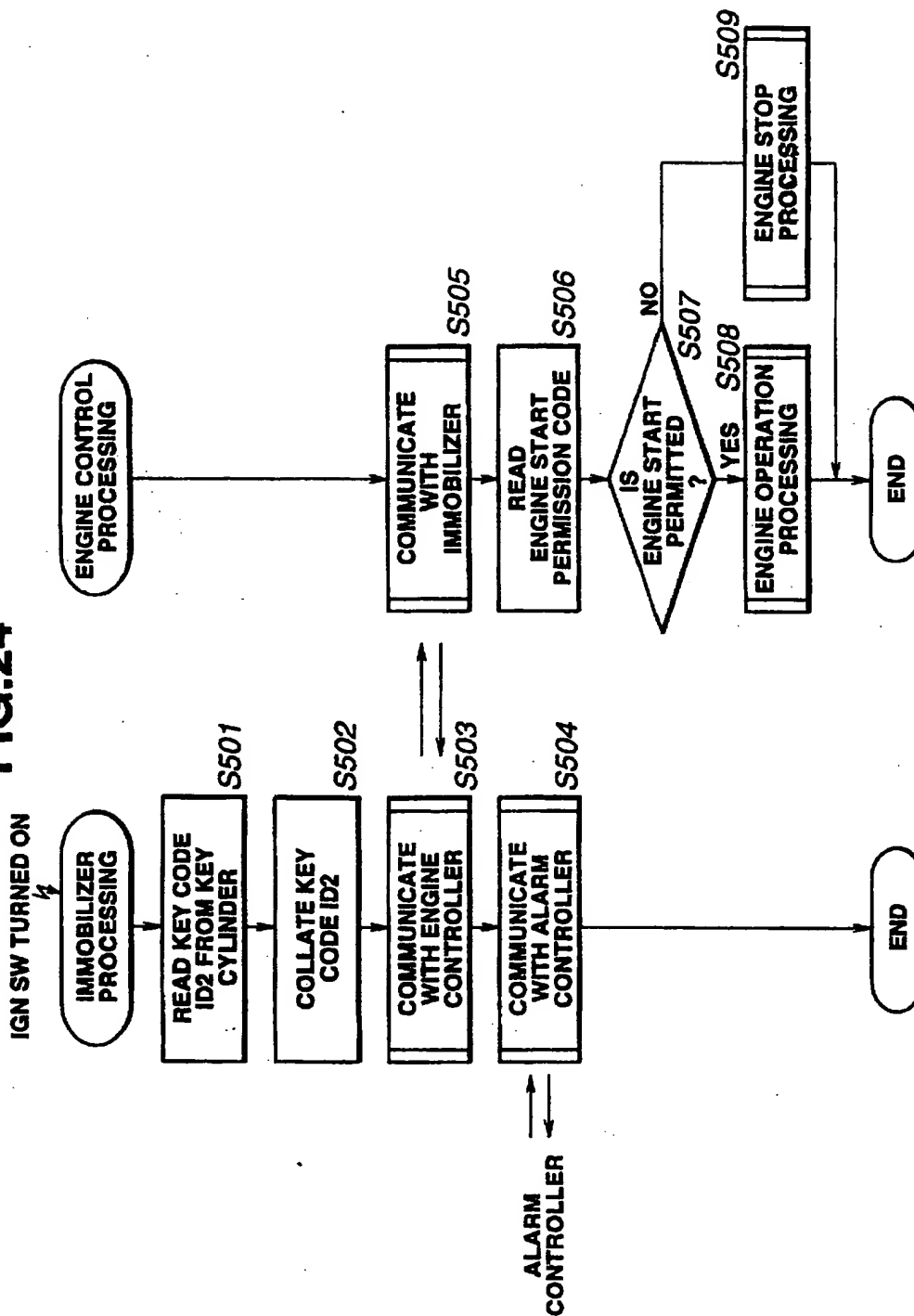


FIG. 24



## ANTI-THEFT CAR PROTECTION SYSTEM

## BACKGROUND OF THE INVENTION

The present invention relates generally to an anti-theft car protection system and more particularly, to the anti-theft car protection system which adopts collation of an ID number of an ignition key.

Various types of anti-theft car protection systems have been proposed in past years to prevent unfair unlocking of a key of a motor vehicle, etc. One is constructed such that an ID number of the key is transmitted when inserting the key into a key cylinder, and start of an engine is permitted only when the ID number coincides with a previously registered one.

A problem encountered in the above conventional anti-theft car protection system is such that if the engine is stopped for some reason after start with coincidence of the ID number, key collation is carried out again, taking time for restart of the engine.

In view of such problem, JP-A 64-56248 proposes a system which, when the engine is stopped for some reason after start, key collation is not carried out upon restart of the engine. More concretely, the system is provided with a holding circuit for continuously holding an engine control unit for controlling start of the engine in a turn-on state, which is in operation once the engine is started, permitting start of the engine without key collation.

In JP-A 64-56248, the holding circuit comprises a transistor, a relay, and a diode, which are connected to a CPU for controlling the entirety of the system and a main relay. Moreover, the holding circuit includes a battery, a key switch to be turned on when the key is operated to an ignition turn-on position, and an engine control unit.

In this holding circuit, with coincidence of the ID number of the key, the CPU outputs a high-level signal to turn on the transistor. In that state, if the key is operated to an ignition turn-on position, the key switch is turned on to pass a current through a coil of the relay, which is also turned on. With the relay turned on, a current passes through a coil of the main relay, which is also turned on, so that the engine control unit is turned on to start the engine.

In that state, even if the CPU outputs a low-level signal, the relay is maintained in a turn-on state due to the diode connected, and therefore, the main relay is also maintained in a turn-on state. That is, once the transistor is turned on, the engine control unit switches operation in accordance with turn-on/turn-off of the key switch regardless of a collation result of the key.

In such a way, the system of JP-A 64-56248 is provided with the holding circuit by which key collation can be avoided upon restart of the engine.

The holding circuit of JP-A 64-56248 serves to hold the relay in a turn-on state even if the CPU breaks down with the key operated to an ignition turn-on position. However, once the key is operated to an ignition turn-off position, holding of the relay by the holding circuit is released. Therefore, if the CPU malfunctions after ignition turn-off to output no signal to the holding circuit, start of the engine is not possible. That is, with the system of JP-A 64-56248, if the CPU malfunctions which carries out key collation, start of the engine is impossible even if the key is operated to an ignition turn-off position, then, to an ignition turn-on position again.

It is, therefore, an object of the present invention to provide an anti-theft car protection system which is free of

the above drawback, and ensures start of the engine without repetition of key operation and inconvenience with respect to the system itself as long as the key as applied is a formal one.

## SUMMARY OF THE INVENTION

According to one aspect of the present invention, there is provided an anti-theft car protection system for a motor vehicle having an engine, an engine control unit and a key, comprising:

means for receiving a code of the key transmitted therefrom;

means for collating said code as received with a code as registered, and transmitting an engine start permission signal to the engine control unit when said code as received coincides with said code as registered; and

means, cooperating with said code collating means, for removing repetition of key operation upon start of the engine.

According to another aspect of the present invention, there is provided a method of protecting a motor vehicle from a theft, the motor vehicle having an engine, a key, an engine control unit and an immobilizer unit, the method comprising the steps of:

receiving a code of the key transmitted therefrom;

collating said code as received with a code as registered;

transmitting an engine start permission signal to the engine control unit when said code as received coincides with said code as registered; and

removing repetition of key operation upon start of the engine.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing a first preferred embodiment of an anti-theft car protection system according to the present invention;

FIG. 2A is a view similar to FIG. 1, showing a transmitter-receiver arranged in a motor vehicle;

FIG. 2B is a view similar to FIG. 2A, showing a transponder built in a key;

FIG. 3 is a view similar to FIG. 2B, showing connection between input and output terminals of the transmitter-receiver, an immobilizer control unit, and an engine control unit;

FIG. 4 is a flowchart showing operation of the immobilizer control unit upon ignition turn-on;

FIG. 5 is a view similar to FIG. 4, showing operation of the engine control unit upon ignition turn-on;

FIG. 6 is a view similar to FIG. 5, showing operation of the immobilizer control unit upon ignition turn-off;

FIG. 7 is a view similar to FIG. 6, showing operation of the engine control unit upon ignition turn-off;

FIG. 8 is a view similar to FIG. 3, showing a second preferred embodiment of the present invention;

FIG. 9 is a perspective view illustrating a key;

FIG. 10 is a view similar to FIG. 7, showing operation of the engine control unit of FIG. 8;

FIG. 11 is a view similar to FIG. 10, showing operation of the engine control unit subsequent to FIG. 10;

FIG. 12 is a view similar to FIG. 11, showing a third preferred embodiment of the present invention;

FIG. 13 is a view similar to FIG. 8, showing a fourth preferred embodiment of the present invention;



FIG. 14 is a view similar to FIG. 9, illustrating the key;

FIG. 15 is a view similar to FIG. 12, showing an operation permission processing program of the engine control unit;

FIG. 16 is a view similar to FIG. 15, showing an engine stop processing program of the engine control unit;

FIG. 17 is a view similar to FIG. 16, showing an ID collation processing program of the immobilizer unit;

FIG. 18 is a view similar to FIG. 17, showing a connector disconnection interrupt routine of the engine control unit;

FIG. 19 is a view similar to FIG. 18, showing a connector connection interrupt routine of the engine control unit;

FIG. 20 is a view similar to FIG. 14, illustrating a motor vehicle to which a fifth preferred embodiment of the present invention is applied;

FIG. 21 is a view similar to FIG. 13, showing a fifth preferred embodiment of the present invention;

FIG. 22 is a view similar to FIG. 19, showing a remote locking/unlocking control processing carried out between a portable equipment and a locking/unlocking and alarm control unit;

FIG. 23 is a view similar to FIG. 22, showing an alarm control processing of the locking/unlocking and alarm control unit; and

FIG. 24 is a view similar to FIG. 23, showing an engine start processing.

#### DETAILED DESCRIPTION OF THE INVENTION

Referring to the drawings, preferred embodiments of an anti-theft car protection system will be described.

FIGS. 1-7 show a first embodiment of the present invention. Referring to FIG. 1, an anti-theft car protection system comprises a key 1 having a transponder 11 built therein for ensuring transmission/receiving with respect to a vehicular antenna 2. Referring to FIG. 2B, the transponder 11 comprises a charge converter 101 for accumulating in a capacitor, not shown, radio waves derived from the vehicular antenna 2 and received by a key antenna 12 in the form of an electric charge, an EEPROM 102 for storing the ID number of the key 1, and a controller 103 for controlling read-out of the ID number, transmission/receiving of radio waves with respect to a motor vehicle, etc.

Referring again to FIG. 1, a transmitter-receiver 3 is provided for ensuring transmission/receiving with respect to the key 1. Referring to FIG. 2A, the transmitter-receiver 3 comprises a transmission/receiving switch 31 for switching transmission/receiving of radio waves, a capacitor 33 for accumulating received radio waves in the form of an electric charge, a demodulator 34 for demodulating received waves, and a transmission controller 35 for controlling a timing of transmit of radio waves, etc.

Referring again to FIG. 1, an immobilizer control unit 4 is provided for detecting whether or not the ID number of the key 1 coincides with a previously registered code. The immobilizer control unit 4 carries out key collation when the key 1 is operated to an ignition turn-on position, and transmits, when the ID number coincides with the code, an engine start permission signal to an engine control unit 5. The engine control unit 5 starts an engine, not shown, when receiving the engine start permission signal from the immobilizer control unit 4.

FIG. 3 is a block diagram showing connection between input and output terminals of the transmitter-receiver 3, the immobilizer control unit 4, and the engine control unit 5 as

shown in FIG. 1. Referring to FIG. 3, the transmitter-receiver 3 and the immobilizer control unit 4 are interconnected by a power source terminal B, a ground terminal GND, a terminal TX of transmit data to the key 1, and a terminal RX of receive data from the key 1. The immobilizer control unit 4 and the engine control unit 5 are interconnected by a terminal TX of a start signal from the immobilizer control unit 4 and a terminal RX of an engine start state signal from the engine control unit 5. The immobilizer control unit 4 is provided with a terminal BAT of a source voltage from a battery, not shown, a terminal ACC of an ACC switch to be turned on when the key 1 is operated to an accessory position, a terminal IGN of an IGN switch to be turned on when the key 1 is operated to an ignition turn-on position, and a terminal ST of a ST switch to be turned on when the key 1 is operated to a start position.

Referring to FIGS. 1-7, operation of the first embodiment will be described.

FIG. 4 is a flowchart showing operation of the immobilizer control unit 4 when the key 1 is operated to an ignition turn-on position.

Referring to FIG. 4, at a step S1, the vehicular antenna 2 transmits radio waves of, e.g. 120 kHz to the key 1. The radio waves are received by the key antenna 12, and input to the charge converter 101 of the transponder 11 for rectification, which are then accumulated in the capacitor in the form of an electric charge. The charge converter 101 converts an accumulated charge into a voltage which is supplied to power source terminals B of the EEPROM 102 and the controller 103. The controller 103 transmits an ID number read out of the EEPROM 102 to the charge converter 101 which in turn transmits the ID number to the vehicular antenna 2.

At a step S2, the ID number transmitted from the key 1 is received. That is, the ID number is read which is received by the vehicular antenna 2, and demodulated by the demodulator 34 of the transmitter-receiver 3.

At a step 3, it is determined whether or not the ID number transmitted from the key 1 corresponds to a previously registered one. If determination is affirmative, control proceeds to a step S4 where a code indicative of an engine start permission signal is transmitted to the engine control unit 5. The code indicative of an engine start permission signal is transmitted from the engine control unit 5 to the immobilizer control unit 4 as will be described later.

On the other hand, at the step S3, if determination is negative, control proceeds to a step S5 where a code indicative of an engine start prohibition signal is transmitted to the engine control unit 5. The code indicative of an engine start prohibition signal is also transmitted from the engine control unit 5 to the immobilizer control unit 4.

FIG. 5 is a flowchart showing operation of the engine control unit 5 when the key 1 is operated to an ignition turn-on position. Referring to FIG. 5, at a step S11, it is determined whether or not a collation result OK flag is set. The collation result OK flag is a flag indicative that the code transmitted from the immobilizer control unit 4 coincides with the code indicative of an engine start permission signal, and set when the former code coincides with the latter code. A value of the collation result OK flag is stored in an EEPROM, not shown, of the engine control unit 5.

At the step S11, if determination is negative, control proceeds to a step S12 where the code transmitted from the immobilizer control unit 4 is received. At a subsequent step S13, it is determined whether or not the received code corresponds to the code indicative of an engine start per-

mission signal. If determination is affirmative, control proceeds to a step S14 where engine start control is carried out, then, it comes to an end.

On the other hand, at the step S13, if determination is negative, control proceeds to a step S15 where engine stop control is carried out, then, it comes to an end.

At the step S11, if determination is affirmative, control proceeds to the step S14. That is, when the collation result OK flag is already set, an engine is started regardless of a code collation result.

The above operation of the immobilizer control unit 4 and the engine control unit 5 upon ignition turn-on will be described in brief. The immobilizer control unit 4 collates the ID number transmitted from the key 1 with the previously registered number. If the former number coincides with the latter number, the immobilizer control unit 4 transmits the code indicative of an engine start permission signal to the engine control unit 5. The engine control unit 5 determines whether or not the code indicative of an engine start permission signal is received. If determination is affirmative, the collation result OK flag to be stored in the EEPROM is set. On the other hand, when the collation result OK signal is already set upon ignition turn-on, the engine control unit 5 permits engine start without detecting the code from the immobilizer control unit 4.

In such a way, if the collation result OK flag is set, engine start is permitted regardless of a key collation result. In case that the immobilizer control unit 4 or the engine control unit 5 malfunctions after the key collation result is affirmative, the engine is started in accordance with a result of conventional mechanical key collation such as comparison of a key shape, etc. regardless of a result of electrical key collation ensured by the immobilizer control unit 4.

FIG. 6 is a flowchart showing operation of the immobilizer control unit 4 when the key 1 is operated to an ignition turn-off position.

Referring to FIG. 6, at a step S21, the code is received which is indicative of an engine start permission signal transmitted from the engine control unit 5. The received code is used upon subsequent ignition turn-on. That is, when transmitting an engine start permission signal to the engine control unit 5, the code received at the step S21 is transmitted to the engine control unit 5. At a subsequent step S22, the code received at the step S21 is returned to the engine control unit 5, and control comes to an end.

The reason why the code received once is returned to the engine control unit 5 in such a way is to determine through transmission/receiving of the code whether or not communication between the immobilizer control unit 4 and the engine control unit 5 is carried out correctly.

FIG. 7 is a flowchart showing operation of the engine control unit 5 when the key 1 is operated to an ignition turn-off position.

Referring to FIG. 7, at a step S31, a variable N is initialized to 0. The variable N serves to measure the number of times of execution of control at a step S33 as will be described later. At a subsequent step S32, a new code indicative of an engine start permission signal is transmitted to the immobilizer control unit 4. The reason why the new code indicative of an engine start permission signal is transmitted every ignition turn-off is to increase an anti-theft performance by changeability of the code indicative of an engine start permission signal.

At the step S33, the code is received which is transmitted from the immobilizer control unit 4. At a subsequent step

S34, it is determined whether or not the received code coincides with the code transmitted at the step S32. If determination is affirmative, control proceeds to a step S35 where the collation result OK flag stored in the EEPROM of the engine control unit 5 is reset, and it comes to an end.

At the step S34, if determination is negative, control proceeds to a step S36 where 1 is added to the variable N. At a subsequent step S37, it is determined whether or not the variable N is greater than a predetermined threshold value L. If determination is negative, control returns to the step S32, whereas if determination is affirmative, control comes to an end.

The above operation of the immobilizer control unit 4 and the engine control unit 5 upon ignition turn-off will be described in brief. The engine control unit 5 transmits the new code indicative of an engine start permission signal to the immobilizer control unit 4. When receiving the new code, the immobilizer control unit 4 returns it to the engine control unit 5. The engine control unit 5 determines whether or not the returned code coincides with the code transmitted to the immobilizer control unit 4. If determination is affirmative, the collation result OK flag is reset which is stored in the EEPROM of the engine control unit 5. On the other hand, if determination is negative, control of coincidence determination is repeatedly carried out L times. With all repetition, if the returned code does not coincide with the code transmitted to the immobilizer control unit 4, control comes to an end.

In such a way, the engine control unit 5 transmits every ignition turn-off the new code indicative of an engine start permission signal to the immobilizer control unit 4, resulting in a further improvement of an anti-theft performance. Further, when the engine control unit 5 transmits the code to the immobilizer control unit 4, the immobilizer control unit 4 returns the code to the engine control unit 5 to check whether or not the code is transmitted correctly. If the code is not transmitted correctly, it is determined that the immobilizer control unit 4 or the engine control unit 5 malfunctions. Thus, malfunction of the immobilizer control unit 4 or the engine control unit 5 can be detected quickly and easily.

Moreover, when the code is not transmitted correctly, the collation result OK flag stored in the EEPROM of the engine control unit 5 is maintained in a set state, so that upon subsequent ignition turn-on, the engine can be started in accordance with a result of mechanical key collation without carrying out electrical key collation in the immobilizer control unit 5.

Thus, even if impossible normal communication or so-called system anomaly occurs in any of the key 1, vehicular antenna 2, transmitter-receiver 3, immobilizer control unit 4, and engine control unit 5 after key collation is OK, the engine can be started. It is noted that "impossible normal communication" corresponds to impossible normal transmission of the ID number of the key 1, the code indicative of an engine start permission signal and the collation result OK flag, impossible normal execution of read and write of a memory such as EEPROM, etc.

On the other hand, when the code is transmitted correctly, the collation result OK flag is reset, then, key collation is carried out again upon ignition turn-on, fulfilling the function of the anti-theft car protection system.

At the steps S33, S34 as shown in FIG. 7, it is determined that malfunction of the immobilizer control unit 4 or the engine control unit 5 occurs when the code which the engine control unit 5 transmits to the immobilizer control unit 4 does not coincide with the code which the latter unit 4

returns to the former unit 5. However, control as shown in FIG. 7 is not limitative as means for detecting whether or not the immobilizer control unit 4 or the engine control unit 5 malfunctions.

Moreover, the condition of resetting the collation result OK flag is not limited to when determination at the step S88 as shown in FIG. 7 is affirmative. By way of example, the collation result OK flag may be reset when an external diagnostic device provides an initializing signal after replacement or repair of a failed portion.

FIGS. 8-11 show a second embodiment of the present invention. Referring to FIG. 8, the anti-theft car protection system comprises a transponder 201, an antenna unit 202, an immobilizer unit 203, and an engine control unit 205.

Referring also to FIG. 9, the transponder 201 is embedded in a head portion 204a of a key 204, and is provided with a nonvolatile memory 211 such as EEPROM in which an ID number of the key 204 is previously stored, a control circuit 212 for controlling communication with the antenna unit 202, and an interface 214 for ensuring communication with the antenna unit 202 through an antenna 213. The interface 214 includes a capacitor, and serves to receive and rectify pulse-signal waves of a predetermined frequency, which is accumulated in the capacitor so as to serve as a power upon ID number transmission. When receiving pulse-signal waves of a predetermined frequency from the antenna unit 202, the control circuit 212 reads the ID number out of the memory 211 by using a power of pulse-signal waves, which is transmitted to the antenna unit 202 of the motor vehicle through the interface 214.

The antenna unit 202 is arranged in an ignition key cylinder, not shown, of the motor vehicle, and is provided with an oscillator 222 for generating a pulse signal of a predetermined frequency to be transmitted to the transponder 201, an amplifier 223 for amplifying a signal received from the transponder 201, a demodulator 224 for demodulating the received signal to the ID number, a switch 225 for connecting the oscillator 222 to the antenna 221 upon signal transmission, and the amplifier 223 to the antenna 221 upon signal receiving, a control circuit 226 for controlling communication with the transponder 201 in accordance with a command out of the immobilizer unit 203, and an interface 227 for ensuring communication with the immobilizer unit 203. When receiving a power transmission command out of the immobilizer unit 223 through the interface 227, the control circuit 226 changes the switch 225 to a contact T so as to transmit to the transponder 201 through the antenna 221 a pulse signal of a predetermined frequency generated by the oscillator 222 during a predetermined period of time. This transmission time is determined to be sufficient for accumulating a transmission power in the interface 214 of the transponder 201. As soon as transmission is completed, the switch 225 is changed to a contact R so as to receive signal waves transmitted by the transponder 201, which are amplified by the amplifier 223, and demodulated to the ID number through the demodulator 224.

The immobilizer unit 203 comprises a microcomputer, not shown, and peripheral parts such as a nonvolatile memory 231, interfaces 232, 233, etc., and serves to ensure communication with the antenna unit 202 through the interface 233 in response to an ID collation request out of the engine control unit 205, and read the ID number of the key 204 through the antenna unit 202, which is collated with that one as previously registered in the memory 281. Moreover, the immobilizer unit 203 ensures communication with the engine control unit 205 through the interface 282 so as to

transmit a collation result of the ID number in response to an ID collation request of the engine control unit 205.

The engine control unit 205 comprises a microcomputer, not shown, and peripheral parts such as an interface 251, a switch 252, etc., and serves to carry out start, stop and speed adjusting of an engine, not shown, and ensure communication with the immobilizer unit 203 through the interface 251 to request ID number collation and receive a result thereof. When receiving an ID noncoincidence signal from the immobilizer unit 203, the engine control unit 205 stops not only operation of a fuel supply system, not shown, for supplying fuel to the engine, but operation of an ignition controller, not shown, for carrying out ignition control of the engine, thus stopping the engine. Ordinarily, the engine control unit 205 closes the switch 252 to permit activation of a starter drive circuit 206 for starting the engine, whereas when it is determined that normal start operation of the engine is not carried out as will be described later, the engine control unit 205 opens the switch 252 to prevent activation of the starter drive circuit 206, thus prohibiting start of the engine.

Connected to the engine control unit 205 are a switch 253 which is closed when the key 204 is set to an engine start position ST, and a speed detector 254 for detecting a cruising speed V of the motor vehicle.

Communication between the immobilizer unit 203 and the engine control unit 205 with regard to ID collation is ensured in accordance with the following procedure:

#### 1) ID collation request

When detecting through the switch 253 that engine start operation is made by the key 204, the engine control unit 205 actuates a starter, fuel supply system, and ignition controller to start the engine, and transmits an ID collation request signal to the immobilizer unit 203.

#### 2) ID coincidence/noncoincidence signal

When receiving an ID collation request signal from the engine control unit 205, the immobilizer unit 203 reads the ID number from the transponder 201 of the key 204 through the antenna unit 202, which is collated with that one as previously registered. In connection with a collation result, the immobilizer unit 203 transmits an ID coincidence signal or ID noncoincidence signal to the engine control unit 205.

When receiving an ID noncoincidence signal from the immobilizer unit 203, the engine control unit 205 stops immediately the fuel supply system and the ignition controller as described above, stopping the engine.

On the other hand, when receiving an ID coincidence signal, the engine control unit 205 confirms whether or not the immobilizer unit 203 itself is formal in accordance with the following procedure without immediately carrying out engine operation permission processing:

#### 3) Rolling code transmission request

The engine control unit 205, which received an ID coincidence signal from the immobilizer unit 203, requests transmission of a rolling code from the immobilizer unit 203. This rolling code is set by the engine control unit 205 upon previous engine stop, and is transmitted to the immobilizer unit 203 for store in the memory 231.

#### 4) Transmission of rolling code

The immobilizer unit 203, which received a rolling code transmission request from the engine control unit 205, transmits to the engine control unit 205 the rolling code received from the engine control unit 205 upon previous engine stop and stored in the memory 231.

The engine control unit 205, which received the rolling code from the immobilizer unit 203, collates the rolling code

with that one transmitted to the immobilizer unit 203 upon previous engine stop. If the two coincide, the engine control unit 205 determines that the immobilizer unit 203 itself is formal, and proceeds to engine operation permission processing. On the other hand, if the two do not coincide, the engine control unit 205 determines that the immobilizer unit 203 or the engine control unit 205 is replaced through a theft, and proceeds immediately to the above engine stop processing, and engine start prohibition processing.

Therefore, a rolling code signal which the immobilizer unit 203 transmits to the engine control unit 205 constitutes substantially an engine operation permission signal, and is referred hereafter to as operation permission signal.

It is noted that the operation permission signal is a signal for permitting continuous operation of the engine which is in operation, and not a signal for permitting start of the engine which is at a standstill.

It is also noted that the ID noncoincidence signal is a signal for stopping the engine which is in operation, and not a signal for prohibiting start of the engine which is at a standstill. A method of stopping engine operation is not limited to a method of stopping operation of the fuel supply system, and a method of stopping operation of ignition controller.

It is also noted that engine start permission means that start of the engine which is at a standstill is permitted, and that engine start prohibition means that start of the engine which is at a standstill is prohibited. These engine start permission and prohibition are invalid for the engine which is already in operation.

The starter drive circuit 206 is a circuit for actuating, when the key 204 is set to the engine start position ST, a starter motor 264 so as to start the engine. The switch 252 is ordinarily closed to permit engine start, so that when closing an ignition start switch 262, a current passes from a battery BAT to a relay coil 263c through a fuse 261, turning on a relay 263. Thus, a relay contact 263a is closed to supply a power from the battery BAT to the starter motor 264 through the fuse 261, ignition start switch 262, and relay contact 263a, actuating the starter motor 264. As described above, when determining that normal start operation of the engine is not carried out, the engine control unit 205 opens the switch 252, so that the relay 263 is turned off to open the relay contact 263a, preventing actuation of the starter motor 264. Therefore, the engine cannot be started.

FIGS. 10 and 11 are flowcharts showing operation of the engine control unit 205. Referring to FIGS. 10 and 11, operation of the second embodiment will be described.

When the switch 253 is closed through engine start operation by the key 204, the engine control unit 205 starts control as shown in FIGS. 10 and 11. At a step S101, a counter is incremented which counts a number of times that the switch 253 is closed, i.e. a number of times L of engine start operation by the key 204, then, control proceeds to a step S102 where it is determined whether or not the cruising speed V of the motor vehicle detected by the speed detector 254 is greater than a predetermined speed M (km/h). If the cruising speed V is greater than the predetermined speed M, control proceeds to a step S103, whereas if not, control proceeds to a step S104. When the cruising speed V is greater than the predetermined speed M, it is determined at the step S103 whether or not the count number L of the counter is equal to or greater than a predetermined number L<sub>0</sub>, i.e. the number of times L of engine start operation by the key 204 comes to the predetermined number L<sub>0</sub>. If L  $\geq$  L<sub>0</sub>, control proceeds to a step S111, whereas if not, control comes to an end.

On the other hand, at the step S102, if it is determined that the cruising speed V is smaller than the predetermined speed M, control proceeds to a step S104 where the ID collation request signal is transmitted to the immobilizer unit 203. At a subsequent step S105, it is determined whether or not the rolling code or operation permission signal is received from the immobilizer unit 203. If the operation permission signal is received, control proceeds to a step S109, whereas if not, control proceeds to a step S106.

When the immobilizer unit 203 transmits the ID noncoincidence signal in connection with an ID collation request, it is determined that engine start operation was carried out by the key 204 with the ID number not registered, so that at the step S106, a counter is incremented which counts a number of times N of noncoincidence of the ID number, and control proceeds to a step S107. At the step S107, it is determined whether or not the count number N of the counter is equal to or greater than a predetermined number N<sub>0</sub>, i.e. the number of times N of noncoincidence of the ID number comes to the predetermined number N<sub>0</sub>. If N  $\geq$  N<sub>0</sub>, control proceeds to the step S111, whereas if not, control proceeds to a step S108.

At the step S108, due to receiving of the ID noncoincidence signal, the fuel supply system and the ignition controller are stopped to stop the engine which is in operation.

On the other hand, when receiving the operation permission signal from the immobilizer unit 203, it is determined that the key 204 used for engine start operation is a registered key, and that the immobilizer unit 203 is formal, so that at the step S109, the count numbers N, L are reset to 0. At a subsequent step S110, engine operation is permitted.

When the cruising speed V is greater than the predetermined speed M, and the number of times L of engine start operation comes to the predetermined number L<sub>0</sub>, or when the number of times N of noncoincidence of the ID number comes to the predetermined number N<sub>0</sub>, it is determined that normal start operation of the engine is not carried out, so that at the step S111, engine start is prohibited. That is, as described above, the switch 252 is opened to prohibit actuation of the starter motor 264. It is noted that at that time, operation of the fuel supply system and the ignition controller may be stopped simultaneously. At a subsequent step S112, an ID collation request to the immobilizer unit 203 is stopped to stop ID number collation by the immobilizer unit 203.

At a subsequent step S113, it is determined whether or not prohibition of engine start and stop of ID number collation are continued during T hours. If T hours elapse, control proceeds to a step S114, whereas if not, control returns to the step S111. When prohibition of engine start and stop of ID number collation are continued during T hours, at the step S114, not only the count numbers N, L are reset to 0, but the switch 252 is closed, and control comes to an end. Thus, prohibition of engine start and stop of ID collation are released after T hours, permitting engine start operation by the key 204 again.

In such a way, with the anti-theft car protection system which gives priority to engine start up to completion of ID number collation, when detecting the cruising speed over a predetermined speed, and having the number of times of engine start operation equal to a predetermined number, not only ID number collation is stopped, but engine start is prohibited during a predetermined period of time, resulting in prevention of wastefully consumed power of the battery by repetition of engine start due to the use of a key other than the formal key such as a sub key, and improvement of the

anti-theft performance due to stop of ID number collation during a predetermined period of time.

Moreover, with the anti-theft car protection system which gives priority to engine start up to completion of ID number collation, when having the number of times of noncoincidence of the ID number equal to a predetermined number, not only ID number collation is stopped, but engine start is prohibited during a predetermined period of time, resulting in the same effect as described above.

FIG. 12 shows a third embodiment of the present invention. In the second embodiment, in order to avoid a waiting of engine start up to completion of ID number collation, engine start has priority up to completion of ID number collation, and engine operation permission or stop is carried out in accordance with a collation result upon completion of ID number collation. On the other hand, in the third embodiment, engine start is not permitted up to completion of ID number collation at the sacrifice of startability of the engine, and engine start permission or prohibition is carried out in accordance with a collation result upon completion of ID number collation.

The structure of the third embodiment is substantially the same as that of the second embodiment as shown in FIGS. 8 and 9.

In the third embodiment, the engine control unit 205 opens the switch 252 ordinarily, and closes it when receiving an engine operation permission signal from the immobilizer unit 203. That is, the engine control unit 205 prohibits actuation of the starter motor 264 until the immobilizer unit 203 transmits an engine operation permission signal.

FIG. 12 is a flowchart showing operation of the engine control unit 205. Referring to FIG. 12, operation of the third embodiment will be described.

When the switch 253 is closed through engine start operation by the key 204, the microcomputer of the engine control unit 205 starts control as shown in FIG. 12. At a step S121, even if the key 204 is turned to the engine start position ST, engine start is prohibited with the switch 252 opened. As described above, in the third embodiment, since the engine control unit 205 does not close the switch 252 up to receiving of an engine operation permission signal, and actuation of the starter motor 264 is prohibited, the engine is not started. It is noted that at that time, the fuel supply system and the ignition controller may be stopped simultaneously.

At a step S122, an ID collation request signal is transmitted to the immobilizer unit 203, and at a subsequent step S123, it is determined whether or not the rolling code or engine operation permission signal is received from the immobilizer unit 203. When the engine operation permission signal is received from the immobilizer unit 203, control proceeds to a step S124, whereas if not, control proceeds to a step S127.

When the engine operation permission signal is received from the immobilizer unit 203, it is determined that the key 204 used for engine start operation is a registered key, and that the immobilizer unit 203 is formal, and the count number N of the counter for counting a number of times of noncoincidence of the ID number is reset to 0. At a subsequent step S125, the switch 252 is closed to allow actuation of the starter motor 264, permitting engine start. Then, control comes to an end.

On the other hand, when receiving an ID noncoincidence signal, at the step S127, the count number N of the counter is incremented, and at a subsequent step S128, it is determined whether or not the count number N comes to the

predetermined number No, i.e. the number of times N of noncoincidence of comes to the predetermined number No. If  $N \geq No$ , control proceeds to a step S129, whereas if not, control comes to an end.

When the ID noncoincidence number N comes to the predetermined number No, at the step S129, an ID collation request to the immobilizer unit 203 is stopped to stop ID collation by the immobilizer unit 203. At a subsequent step S130, it is determined whether or not stop of ID collation is continued during T hours. If T hours elapse, control proceeds to a step S131, whereas if not, control returns to the step S129. When stop of ID collation is continued during T hours, at the step S131, the count number N is reset to 0, and control comes to an end.

In such a way, with the anti-theft car protection system which prohibits engine start up to completion of ID number collation, when having the number of times of noncoincidence of ID number equal to a predetermined number, ID number collation is stopped during a predetermined period of time, resulting in prevention of wastefully consumed power of the battery by repetition of engine start due to the use of a key other than the formal key such as a sub key, and improvement of the anti-theft performance due to stop of ID number collation during a predetermined period of time.

FIGS. 13-19 show a fourth embodiment of the present invention. Referring to FIG. 13, the anti-theft car protection system comprises a transponder 301, an antenna unit 302, an immobilizer unit 303, an engine control unit 305, and a connector 306.

Referring also to FIG. 14, the transponder 301 is embedded in a head portion 304a of a key 304, and is provided with a nonvolatile memory 311 such as EEPROM in which an ID number of the key 304 is previously stored, a control circuit 312 for controlling communication with the antenna unit 302, and an interface 314 for ensuring communication with the antenna unit 302 through an antenna 313. The interface 314 includes a capacitor, and serves to receive and rectify pulse-signal waves of a predetermined frequency, which is accumulated in the capacitor so as to serve as a power upon ID number transmission. When receiving pulse-signal waves of a predetermined frequency from the antenna unit 302, the control circuit 312 reads the ID number out of the memory 311 by using a power of pulse-signal waves, which is transmitted to the antenna unit 302 of the motor vehicle through the interface 314.

The antenna unit 302 is arranged in an ignition key cylinder, not shown, of the motor vehicle, and is provided with an oscillator 322 for generating a pulse signal of a predetermined frequency to be transmitted to the transponder 301, an amplifier 323 for amplifying a signal received from the transponder 301, a demodulator 324 for demodulating the received signal to the ID number, a switch 325 for connecting the oscillator 322 to the antenna 321 upon signal transmission, and the amplifier 323 to the antenna 321 upon signal receiving, a control circuit 326 for controlling communication with the transponder 301 in accordance with a command out of the immobilizer unit 303, and an interface 327 for ensuring communication with the immobilizer unit 303. When receiving a power transmission command out of the immobilizer unit 323 through the interface 327, the control circuit 326 changes the switch 325 to a contact T so as to transmit to the transponder 301 through the antenna 321 a pulse signal of a predetermined frequency generated by the oscillator 322 during a predetermined period of time. This transmission time is determined to be sufficient for accumulating a transmission power in the interface 314 of

the transponder 301. As soon as transmission is completed, the switch 325 is changed to a contact R so as to receive signal waves transmitted by the transponder 301, which are amplified by the amplifier 323, and demodulated to the ID number through the demodulator 324.

The immobilizer unit 303 comprises a microcomputer 334 and peripheral parts such as a nonvolatile memory 331, interfaces 332, 333, etc., and serves to ensure communication with the antenna unit 302 through the interface 333 in response to an ID collation request out of the engine control unit 305, and read the ID number of the key 304 through the antenna unit 302, which is collated with that one as previously registered in the memory 331. Moreover, the immobilizer unit 303 ensures communication with the engine control unit 305 through the interface 332 so as to transmit a collation result of the ID number in response to an ID collation request of the engine control unit 305.

The engine control unit 305 is provided with a microcomputer 352, peripheral parts such as an interface 351 and a memory 353, an auxiliary power source capacitor 354, etc., and serves to carry out start, stop and speed adjusting of an engine, not shown, and ensure communication with the immobilizer unit 303 through the interface 351 to request ID number collation and receive a result thereof. When receiving an ID noncoincidence signal from the immobilizer unit 303, the engine control unit 305 stops not only operation of a fuel supply system, not shown, for supplying fuel to the engine, but operation of an ignition controller, not shown, for carrying out ignition control of the engine, thus stopping the engine.

Connected to the engine control unit 305 are the connector 306 for supplying a power out of a battery BAT, a switch 371 which is closed when the key 304 is set to an engine start position ST, and a switch 372 which is closed when the key 304 is set to an engine operation position ON or the engine start position ST. Upon disconnection of the connector 306, the auxiliary power source capacitor 354 supplies a power to the engine control unit 305 during a predetermined period of time so as to continue operation thereof. Arranged in the connector 306 is a jumper 361 for short-circuiting terminals A and B on the side of the engine control unit 305. When the connector 306 is connected to the engine control unit 305, the terminals A and B are short-circuited by the jumper 361, whereas when the connector 306 is disconnected therefrom, the terminals A and B are opened. The terminals A, B are connected to the microcomputer 352. When the terminals A and B are opened, the microcomputer 352 undergoes an interrupt, executing an interrupt routine as will be described later.

Communication between the immobilizer unit 303 and the engine control unit 305 with regard to ID collation is ensured in accordance with the following procedure:

#### 1) ID collation request

When detecting through the switch 371 that engine start operation is made by the key 304, the engine control unit 305 actuates a starter, not shown, fuel supply system, and ignition controller to start the engine, and transmits an ID collation request signal to the immobilizer unit 303.

#### 2) ID coincidence/noncoincidence signal

When receiving an ID collation request signal from the engine control unit 305, the immobilizer unit 303 reads the ID number from the transponder 301 of the key 304 through the antenna unit 302, which is collated with that one as previously registered. In connection with a collation result, the immobilizer unit 303 transmits an ID coincidence signal or ID noncoincidence signal to the engine control unit 305.

When receiving an ID noncoincidence signal from the immobilizer unit 303, the engine control unit 305 stops immediately the fuel supply system and the ignition controller as described above, stopping the engine.

On the other hand, when receiving an ID coincidence signal, the engine control unit 305 confirms whether or not the immobilizer unit 303 itself is formal in accordance with the following procedure without immediately carrying out engine operation permission processing:

#### 3) Rolling code transmission request

The engine control unit 305, which received an ID coincidence signal from the immobilizer unit 303, requests transmission of a rolling code from the immobilizer unit 303. This rolling code is set by the engine control unit 305 upon previous engine stop, and is transmitted to the immobilizer unit 303 for store in the memory 331.

#### 4) Transmission of rolling code

The immobilizer unit 303, which received a rolling code transmission request from the engine control unit 305, transmits to the engine control unit 305 the rolling code received from the engine control unit 305 upon previous engine stop and stored in the memory 331.

The engine control unit 305, which received the rolling code from the immobilizer unit 303, collates the rolling code with that one transmitted to the immobilizer unit 303 upon previous engine stop. If the two coincide, the engine control unit 305 determines that the immobilizer unit 303 itself is formal, and proceeds to engine operation permission processing. On the other hand, if the two do not coincide, the engine control unit 305 determines that the immobilizer unit 303 or the engine control unit 305 is replaced through a theft, and proceeds immediately to the above engine stop processing, and engine start prohibition processing.

Therefore, a rolling code signal which the immobilizer unit 303 transmits to the engine control unit 305 constitutes substantially an engine operation permission signal, and is referred hereafter to as operation permission signal.

The memory 353 of the engine control unit 305 is a nonvolatile memory such as EPROM, and serves to store a rolling code, i.e. an engine operation permission signal, transmitted from the immobilizer unit 303.

It is noted that the engine operation permission signal is a signal for permitting continuous operation of the engine which is in operation, and not a signal for permitting start of the engine which is at a standstill.

It is also noted that the ID noncoincidence signal is a signal for stopping the engine which is in operation, and not a signal for prohibiting start of the engine which is at a standstill. A method of stopping engine operation is not limited to a method of stopping operation of the fuel supply system, and a method of stopping operation of ignition controller.

It is also noted that engine start permission means that start of the engine which is at a standstill is permitted, and that engine start prohibition means that start of the engine which is at a standstill is prohibited. These engine start permission and prohibition are invalid for the engine which is already in operation.

FIG. 15 is a flowchart showing an operation permission processing program of the engine control unit 305. Referring to FIG. 15, an operation permission processing of the engine control unit 305 will be described.

When detecting through the switch 371 that an engine start operation is carried out by the key 304, the microcomputer 352 of the engine control unit 305 starts execution of



the program. At a step S210, ID number collation of the key 304 used for start operation is requested of the immobilizer unit 303. At a subsequent step S212, it is determined whether or not an ID coincidence signal is received from the immobilizer unit 303. If the ID coincidence signal is received, an operation permission processing after a step S214 is carried out. On the other hand, if an ID noncoincidence signal is received from the immobilizer unit 303, or no response is received therefrom, control proceeds to a step S224 where operation of the fuel supply system and the ignition controller is stopped to stop the engine.

When the ID coincidence signal is received from the immobilizer unit 303 with respect to an ID collation request, at the step S214, transmission of a rolling code is requested of the immobilizer unit 303 so as to confirm whether or not the immobilizer unit 303 and the engine control unit 305 are formal. The rolling code is a code transmitted to the immobilizer unit 303 upon previous engine stop, and stored in the memory 331. At a step S216, it is determined whether or not a rolling code is received from the immobilizer unit 303. If the rolling code is received, control proceeds to a step S218, whereas if not, control proceeds to a step S224 to stop the engine. When receiving the rolling code, at the step S218, the rolling code as received is collated with that one stored in the memory 353 and transmitted to the immobilizer unit 303 upon previous engine stop. If the two coincide, control proceeds to a step S220, whereas if not, control proceeds to the step S224 to stop the engine. At the step S220, due to the fact that the rolling code transmitted to the immobilizer unit 303 upon previous engine stop coincides with that one currently transmitted from the immobilizer unit 303, it is determined that the immobilizer unit 303 and the engine control unit 305 are formal, storing as an operation permission signal the rolling code in the memory 353. At a subsequent step S222, continuous operation of the engine is permitted.

FIG. 16 is a flowchart showing an engine stop processing program of the engine control unit 305. Referring to FIG. 16, an engine stop processing of the engine control unit 305 will be described.

When detecting through the 372 that engine stop operation is carried out by the key 304, the microcomputer 352 of the engine control unit 305 starts execution of the program. At a step S260, update of the rolling code is requested of the immobilizer unit 303, and a new rolling code is transmitted and stored in the memory 353. A code read at random out of a plurality of codes stored in the memory 353 serves as a rolling code.

The immobilizer unit 303 which receives a rolling code update request stores the new rolling code sequentially transmitted, which is returned to the engine control unit 305 so as to notify completion of a rolling code update processing.

At a step S262, the new rolling code returned from the immobilizer unit 303 is received, and collated with the rolling code transmitted previously for update. At a subsequent step S264, it is determined whether or not the two coincide. If the two coincide, control proceeds to a step S266, whereas if not, control proceeds to a step S268. When the rolling code transmitted for update coincides with the new one returned from the immobilizer unit 303, it is determined that update of the rolling code is completed in the immobilizer unit 303 and the engine control unit 305, and at the step S266, the new rolling code is stored as an operation permission signal in the memory 353.

On the other hand, when the rolling code as transmitted does not coincide with the new one as returned, it is

determined that update of the rolling code is not completed, and at the step S268, a number of times N of noncoincidence is incremented. At a subsequent step S270, it is determined whether or not the noncoincidence number N is equal to or greater than a predetermined number L. If  $N \geq L$ , control proceeds to a step S272 where an alarm is given, then, control comes to an end. On the other hand, if  $N < L$ , control returns to the step S260 to repeat the above engine stop processing.

FIG. 17 is a flowchart showing an ID collation processing program of the immobilizer unit 303. Referring to FIG. 17, an ID collation processing will be described.

When detecting through the switch 372 that the key 304 is set to the engine start position ST or the engine operation position ON, the microcomputer 334 of the immobilizer unit 303 starts execution of the program.

At a step S230, it is determined whether or not an ID collation request is made out of the engine control unit 305. If an ID collation request is made, control proceeds to a step S232, whereas if not, control proceeds to a step S244. When an ID collation request is made, at the step S232, an ID number set in the transponder 301 of the key 304 is read through the antenna unit 302 as described above, and is collated with a registered number stored in the memory 331. At a subsequent step S234, it is determined whether or not the ID number of the key 304 which is being applied coincides with the registered number. If the ID number coincides with the registered number, control proceeds to a step S236, whereas if not, control proceeds to a step S238.

When the key 304 which is being applied corresponds to the registered key, at the step S236, an ID coincidence signal is transmitted to the engine control unit 305. At a subsequent step S240, it is determined whether or not a rolling code transmission request is made from the engine control unit 305. If a rolling code transmission request is made, control proceeds to a step S242, whereas if not, control proceeds to the step S244. When a rolling code transmission request is made, at the step S242, a rolling code received and stored upon previous engine stop is read out of the memory 331, and transmitted to the engine control unit 305.

On the other hand, when a nonregistered key is being applied, at the step S238, an ID noncoincidence signal is transmitted to the engine control unit 305, then, control proceeds to the step S244.

At the step S244, it is determined whether or not a rolling code update request is made from the engine control unit 305. If a rolling code update request is made, control proceeds to a step S246, whereas if not, control returns to the step S230. When a rolling code update request is made, at the step S246, a new rolling code is received from the engine control unit 305, and stored in the memory 331. At a subsequent step S248, the new rolling code is returned to the engine control unit 305 so as to notify completion of a rolling code update processing.

FIG. 18 is a flowchart showing a connector disconnection interrupt routine of the engine control unit 305.

When the connector 306 of the engine control unit 305 is disconnected, the terminals A and B are opened as described above. Thus, the microcomputer 352 of the engine control unit 305 undergoes an interrupt, and executes the interrupt routine. That is, at a step S280, a flag F is set which serves to store disconnection of the connector 306.

FIG. 19 is a flowchart showing a connector connection interrupt routine of the engine control unit 305.

When the connector 306 of the engine control unit 305 is connected to supply a power of the battery BAT to the engine

control unit 305, and the terminals A and B are short-circuited by the jumper 361, the microcomputer 352 of the engine control unit 305 executes the interrupt routine.

At a step S290, it is determined whether or not the connector disconnection flag F is set. If the flag F is set, control proceeds to a step S292, whereas if not, control comes to an end. When the flag F is set, the connector 306 has been disconnected for some reason, so that at the step S292, the rolling code is erased if it is stored as an operation permission signal in the memory 353. At a subsequent step S294, the flag F is reset, then, control comes to an end.

FIGS. 20-24 show a fifth embodiment of the present invention. Referring to FIG. 20, a portable equipment 401 is carried by an owner of the motor vehicle 402 with him at all times. The portable equipment 401 has a rectangular thin casing in which a circuit substrate is arranged having an electronic circuit for returning a proper code as previously fixedly stored to the motor vehicle 402 in response to receiving of a transmission request signal from the motor vehicle. In the fifth embodiment, radiocommunication between the portable equipment 401 and the motor vehicle 402 is ensured through radio waves. The other communication mediums may be used such as ultrasonic waves, infrared rays, and laser beams.

On the other hand, referring to FIG. 21, the motor vehicle 402 includes a locking/unlocking and alarm control unit 404 for carrying out collation of a proper code through a transmission/receiving antenna 403, and conducting setting/resetting of the locking/unlocking and alerted state in response to at least a collation result. The locking/unlocking and alarm control unit 404 is accommodated, for example, inside a hood 405. A processing of radiocommunication ensured between the portable equipment 401 and the locking/unlocking and alarm control unit 404 will be described in detail later in accordance with a flowchart in FIG. 22.

Moreover, the motor vehicle 402 includes a hood switch 406 for detecting the open and closed state of the hood 405, door switches 408 for detecting the open and closed state of doors 407, a trunk switch 410 for detecting the open and closed state of a trunk 409, and key cylinder tamper switches 411 for detecting removal of key cylinders built in the doors 7, by which various acts related to a car theft can be detected. In the fifth embodiment, also built in the door 7 is a lock switch, not shown, for detecting whether or not a door lock is set or released, by which the set and released state of the door lock can be detected. That is, as will be described later, the lock switch detects an act that the door lock is released by inserting a mechanical key into the key cylinder of the door 7. A processing of giving an alarm due to unfair opening of the door, etc. will be described in detail later in accordance with a flowchart in FIG. 23.

Additionally, headlamps 412 of the motor vehicle 402 serve to ensure a visual alarm action, whereas a warning horn 413 thereof serves to ensure an auditory alarm action. Door operation switches 14 mounted to the doors 7 serve to provide an opening/closing command to the doors 7 in case of wireless locking/unlocking thereof by the portable equipment 401. This door opening/closing operation will be also described in detail later in accordance with the flowchart in FIG. 22.

FIG. 21 is a block diagram showing an example of a hardware construction of the anti-theft car protection system.

Referring to FIG. 21, a mechanical key 415 is carried by the owner of the motor vehicle 402 with him at all times, and

is used, as is well known, for start of the engine, opening/closing of the doors and trunk, etc. Built in the mechanical key 415 is a chip 415a having a proper code stored therein. The proper code can be read by high-frequency waves in the electromagnetic-induction way. As is known in various documents, a detail of the chip 415a is not described herein.

A key cylinder 416 is arranged into which the mechanical key 415 is inserted to start the engine. An electromagnetic coil is built in the key cylinder 416 in the way to enclose the mechanical key 415 as inserted, and serves to read, through high-frequency waves passing therethrough, the proper code from the chip 415a of the mechanical key 415.

An immobilizer unit 417 has as a fundamental function to conduct a processing of restrained start of the engine and stop thereof when it is unfairly started by a key switch as directly connected due to destruction of the key cylinder 416. Specifically, the immobilizer unit 417 is controlled globally by a CPU comprising a microprocessor, and can ensure serial communication with the locking/unlocking and alarm control unit 404 and an engine control unit 418 which will be described later.

The engine control unit 418 serves to carry out engine control operation in accordance with signals out of an engine sensor group 419 which is a general term of various sensors necessary to control of the engine, and to output, in response to an operation result, signals necessary to an engine actuator group 420 which is a general term of various actuators necessary to control of the engine. The engine control unit 418 is constructed fundamentally in the same way as in the conventional one except that serial communication can be made with the immobilizer unit 417.

An engine start restraint processing carried out between the immobilizer unit 417 and the engine control unit 418 will be described in detail later in accordance with a flowchart in FIG. 24.

On the other hand, the locking/unlocking and alarm control unit 404 serves to carry out the above wireless locking/unlocking control, and it inputs signals from the switch group 406, 408, 410, 411, 414, and outputs signals to the actuator group 421 comprising a solenoid plunger. In response to alarm output from the locking/unlocking and alarm control unit 404, the headlamps 412 are turned on and off, or the warning horn 413 is driven discontinuously. It is noted that the headlamps 412 may be turned on continuously, or the warning horn 413 may be driven continuously.

Referring to FIG. 22, a detailed description will be made with regard to a remote locking/unlocking control processing carried out between the portable equipment 401 and the locking/unlocking and alarm control unit 404.

In the locking/unlocking and alarm control unit 404 which constitutes a vehicle side equipment, at a step S301, the state of the door operation switch 414 is read at all times.

At a step S302, it is determined whether or not the door 407 is operated. If the door 407 is not operated, control returns to the step S301. On the other hand, if a driver gets out of the motor vehicle 402, and closes the door 407 to actuate the corresponding door operation switch 414, it is determined that the door 407 is operated, and control proceeds to a step S303. At the step S303, a transmission request signal is immediately transmitted to the portable equipment 401 by wireless through the transmission/receiving antenna 403. At a subsequent step S304, it is determined whether or not a proper code ID1 is returned from the portable equipment 401. If the proper code ID1 is not returned, control at the step S304 is repeatedly carried out.



On the other hand, in the portable equipment 401, at a step S313, it is always determined whether or not a transmission request signal is received from the vehicle side equipment. If no transmission request signal is received, control at the step S313 is repeatedly carried out, whereas if a transmission request signal is received, control proceeds to a step S314 where the proper code ID1 is immediately transmitted to the vehicle side equipment by wireless.

Then, in the vehicle side equipment, at the step S304, it is determined that the proper code ID1 is received, and control proceeds to a step S305 where the proper code ID1 of the portable equipment 401 is collated with that of the vehicle side equipment.

At a subsequent step S306, it is determined whether or not the proper code ID1 of the portable equipment 401 is collated with that of the vehicle side equipment. If the two do not coincide, control comes to an end, carrying out no control with regard to locking/unlocking. Then, a vehicle side processing becomes in the state of waiting operation of the door operation switch 414.

On the other hand, at the step S306, if it is determined that the proper code ID1 of the portable equipment 401 is collated with that of the vehicle side equipment, control proceeds to a step S307 where the state of the door lock is immediately read through the lock switch, not shown. At a subsequent step S308, it is determined whether the door lock is set or released. If the door lock is released, control proceeds to a step S309 where a locking processing is carried out to set the door lock by operation of the solenoid plunger built in the door 7. Then, at a step S310, an alarm flag is set to put the motor vehicle in the alerted state.

In such a way, the door lock mounted to the door 407 can be set by simple operation of the door operation switch 414 mounted to the door 407, which is made through a finger of the driver who is an owner of the portable equipment 401, for example. On the other hand, without the portable equipment 401, the door operation switch 414 cannot be operated, never carrying out a locking or unlocking processing.

Similar control is carried out in case that the owner of the motor vehicle 402 releases the door lock of the door 407 when returning to a parking position. That is, subsequent to the step S306 for a proper code coincidence processing, it is determined at the step S308 that the door lock is set, so that control proceeds to a step S311 where a unlocking processing is carried out. Then, at a step S312, an alarm flag is reset to release the door lock, also resetting the alerted state of the motor vehicle 402.

Referring to FIG. 23, an alarm control processing of the locking/unlocking and alarm control unit 404 will be described in detail.

According to this alarm control processing, at a step S401, the state of the alarm flag is read at all times, which is controlled at the steps S310 and S312 in the flowchart in FIG. 22. When the alarm flag is set, the motor vehicle 402 is controlled in the alerted state, whereas when the alarm flag is reset, the motor vehicle 402 is controlled in the unalerted state.

That is, at a step S402, it is determined that the alarm flag is reset, control comes to an end, carrying out no alarm action even with anomaly of mounting, etc. of the hood, 405, door 407, trunk 409, and key cylinder of the motor vehicle 402.

On the other hand, after reading the alarm flag at the step S401, if it is determined at the step S402 that the alarm flag is set, an alert processing is carried out thereafter for provision against a car theft. Specifically, in the alerted state,

the following control is repeatedly carried out: read of the state of the door switches 408 for detecting the open and closed state of the doors 407 at a step S403, read of the state of the hood switch 406 for detecting the open and closed state of the hood 405 at a step S405, read of the state of the trunk switch 410 for detecting the open and closed state of the trunk 409 at a step S407, read of the state of the lock switch, not shown, for detecting the locked and unlocked state of the door lock at a step S409, read of the state of the key cylinder tamper switches (key cylinder installation switches) 411 for detecting the installed state of the key cylinders built in the doors 407 at a step S411.

In that state, when detecting any of opening of the door 407 at a step S404, opening of the hood 405 at a step S406, opening of the trunk 409 at a step S408, unlocking of the door lock at a step S410, and removal of the key cylinder at a step S412, the alarm actions are started immediately at a step S413.

As described above, with the alarm actions, the warning horn 413 is driven discontinuously to produce an alarm sound of considerable volume to those who are around the motor vehicle 402. At the same time, the headlamps 412 are repeatedly turned on and off to produce a visual alarm indication to those who are around the motor vehicle 402. Thus, the auditory and visual alarm actions enable those who are around the motor vehicle 402 to warn an occurrence of some anomaly thereof. Such alarm actions are continued by a timer during a sufficient period of time to allow those who are around the motor vehicle 402 to sense an occurrence of some anomaly thereof. That is, without a subsequent alarm stop processing, the alarm actions are continuously carried out during a considerable period of time regardless of a participant in opening of the door 407, etc. who may be a legal driver or a thief.

Thus, in the fifth embodiment, control of steps S414-S417 is newly added for the driver who lost the portable equipment 401. Specifically, subsequently to start of the alarm actions at the step S413, at the step S414, a communication processing is carried out between the locking/unlocking and alarm control unit 404 and the immobilizer unit 417 to receive a collation result of a proper code as will be described later.

At the step S415, it is determined whether or not a proper code read from the chip 415a of the mechanical key 415 coincides with that of the motor vehicle 402. If the two coincide, i.e. a key code is correct, an alarm stop processing at the step S416, and an alarm flag reset processing at the step S417 are carried out immediately, obtaining stop of the alarm actions, and immediate releasing of the alerted state of the motor vehicle 402. On the other hand, at the step S415, the proper code read from the key cylinder 416 does not coincide with that of the motor vehicle 402, or the proper code itself does not exist, the above alarm stop processing at the step S416 and alarm flag reset processing at the step S417 are skipped, resulting in continuation of the alarm actions during a predetermined period of time set by the timer.

Referring to FIG. 24, a detailed description will be made with regard to operation of the immobilizer unit 417 related to an alarm stop processing at the step S416 and an alarm flag reset processing at the step S417 which feature the present invention.

In the immobilizer unit 417, at a step S501, as soon as an ignition switch is turned on with the key cylinder 416, a proper code ID2 is read from the key cylinder 416. That is, as described above, the chip 415a having a proper code

stored therein is built in the mechanical key 415 applied in the fifth embodiment. When the mechanical key 415 is inserted into the key cylinder 416, and that a key switch constituting the key cylinder is turned to an ignition position, the immobilizer unit 417 is actuated to read the proper code ID2 from the mechanical key 415.

At a subsequent step S502, the proper code ID2 or key code as read is collated with that of the motor vehicle 402. The most common technique of a car theft is a forgery of the mechanical key 415 by copying only the shape thereof, and a destruction of the key cylinder 416 through the door 407 opened by breaking a window glass thereof, the engine being started by directly connecting contacts of the switch built in the key cylinder 416. In case of a car theft employing such technique, due to nonexistence of the proper code ID2, it is determined at the step S502 that a result of a collation processing of the proper code or key code ID2 is negative.

At a subsequent step S503, serial communication is carried out between the immobilizer unit 417 and the engine control unit 418.

On the other hand, in the engine control unit 418, at a step S505, communication is carried out with the immobilizer unit 417 to receive a collation result of the key code ID2. At a subsequent step S506, this collation result is recognized as an engine start permission code.

Then, at a step S507, in accordance with the collation result of the key code ID2, it is determined whether or not engine start is permitted. That is, instead of determining that engine start is permitted only when the proper code ID2 read from the mechanical key 415 coincides with that of the motor vehicle 402, it is determined that engine start is unpermitted when the two do not coincide.

At the step S507, if it is determined that engine start is permitted, control proceeds to a step S508 where a normal engine operation processing is carried out wherein a normal engine control operation is carried out in accordance with various signals read from the engine sensor group 419 to output signals to the engine actuator group 420 comprising an injector, ensuring normal subsequent operation of the engine. On the other hand, at the step S507, if it is determined that engine start is unpermitted, control proceeds to a step S509 where an engine stop processing is carried out to stop signals to the engine actuator group 420 immediately, thus stopping the engine.

In such a way, the immobilizer unit 417 is connected to the engine control unit 418 through a communication line, and it permits normal operation of the engine control unit 418 only when coincidence of the proper codes is confirmed. From this point of view, it can be considered that the immobilizer unit 417 serves to restrain engine start.

On the other hand, in the immobilizer unit 417, upon completion of the above engine start restraint processing, at a step S504, communication is carried out with the locking/unlocking and alarm control unit 404 to transmit thereto the collation result of the key code ID2 obtained at the step S502.

Returning to FIG. 23, in the locking/unlocking and alarm control unit 404, as described above, after execution of an alarm start processing at the step S413, communication is carried out with the immobilizer unit 417 at the step S414 to receive the collation result of the key code ID2.

Then, as described above, at the step S415, if it is determined that the key code ID2 is not correct, an alarm stop processing at the step S416 and an alarm flag reset processing at the step S417 are skipped. On the other hand, if it is determined that key code ID2 is correct, an alarm stop

processing and an alarm flag reset processing are executed immediately to stop the alarm actions, releasing the alerted state of the motor vehicle 402.

In such a way, according to the fifth embodiment, referring to FIG. 22, a locking or unlocking processing (step S309 or S311) and an alarm flag set or reset processing (step S310 or S312) are generally carried out through radiocommunication between the portable equipment 401 and the locking/unlocking and alarm control unit 404.

Moreover, when the alarm flag is set, i.e. the motor vehicle 402 is in the alerted state, referring to FIG. 23, in response to opening of the door 407, hood 405, and trunk 409, unlocking of the door lock, and removal of the key cylinder, discontinuous sounding of the warning horn 413 and turn-on/turn-off of the headlamps 412 are continuously carried out during a predetermined period of time.

Such alarm actions are ensured even when the owner of the motor vehicle 402 who lost the portable equipment 401 releases the door lock with the formal mechanical key 415. As a result, a car theft employing a forgery of the mechanical key 415 by copying only the shape thereof can surely be prevented.

On the other hand, when the owner of the motor vehicle 402 releases the door lock with the formal mechanical key 415, then, inserts it into the key cylinder 416 to turn the ignition switch to the ignition position, the immobilizer unit 417 reads the proper code ID2 which is collated with that of the motor vehicle 402 as shown in FIG. 24. Only when the two coincide, the engine control unit 418 is actuated normally, starting operation of the engine. Moreover, only when coincidence of the proper code ID2 is confirmed in such a way, the locking/unlocking and alarm control unit 404 carries out an alarm stop processing as shown in FIG. 23 to stop immediately the alarm actions of turn-on/turn-off of the headlamps 412 and discontinuous sounding of the warning horn 413.

As a result, when the owner of the motor vehicle 402 who lost the portable equipment 401 releases the door lock of the door 407 with the formal mechanical key 415, then, inserts it into the key cylinder 416 to start the engine, the alarm actions can be stopped immediately, releasing the alerted state of the motor vehicle 402. That is, even when the door 407 is opened with the formal engine start key, the alarm actions are carried out. However, the alarm actions can be stopped as soon as engine start operation is carried out by inserting the mechanical key 415 into the key cylinder 416 for start the engine. Thus, as long as the driver is an owner of the motor vehicle 402, and has the formal engine start key, inconveniences can be avoided such as sounding of the warning horn 413 and turn-on/turn-off of the headlamps 412 during a long period of time. On the other hand, when engine start is tried by unfair means such as a shape forgery of the formal mechanical key 415, and a destruction of the key cylinder 416 through the door 407 opened by breaking a window glass thereof, not only engine start is impossible, but the alarm actions cannot be stopped. It will be thus understood that a car theft employing such unfair technique can surely be prevented in avoiding inconveniences such as sounding of the warning horn 413 and turn-on/turn-off of the headlamps 412 during a long period of time when a participant is an owner of the motor vehicle 402 who lost the portable equipment 401.

Having described the present invention in connection with the preferred embodiments, it is noted that the present invention is not limited thereto, and various modifications and changes can be made without departing the spirit of the present invention.

By way of example, collation of the ID number is carried out by transmitting/receiving radio waves between the key and the vehicular antenna. Alternatively, collation of the ID number may be carried out by detecting a quantity of light passing through the key, or a quantity of current by electromagnetic coupling.

Further, the ID number of the key is read out through radiocommunication. Alternatively, wire communication is applicable to read-out of the ID number wherein a circuit of the key is connected to a read-out circuit of the ignition key cylinder through a contact when inserting the key into the ignition key cylinder. Moreover, optical and magnetic communication systems are applicable to read-out of the ID number.

Furthermore, the present invention is applied to a motor vehicle having an engine as a power source, alternatively, it is applicable to a motor vehicle having a power source other than the engine such as an electric vehicle. In that case, it is recommended to provide a start prohibition command to a control unit of the starter motor when the registered key is not inserted into the ignition key cylinder, or that start operation is carried out repeatedly by a key other than the formal key.

Further, the key cylinder serves as a means for reading the proper code of the mechanical key. Alternatively, a code reader for special purpose may be used. Moreover, the immobilizer unit is not indispensable when considering only stop of the warning horn with respect to a normal action made by the owner of the motor vehicle.

Still further, the proper code used in locking/unlocking control of the door is different from that one used in the immobilizer unit, alternatively, the two may be the same code. It is preferable, however, to use two different codes in view of prevention of a car theft.

Furthermore, locking/unlocking control and alarm control are carried out by the locking/unlocking and alarm control unit, alternatively, they may be ensured by two different units.

What is claimed is:

1. An anti-theft protection system for a motor vehicle having an engine and a key with a transponder comprising:  
means for receiving a code of the key transmitted from the transponder;

means for controlling the engine; and

means for transmitting an engine start permission signal to said engine controlling means when said code as received coincides with code as registered;

said engine controlling means including:

means for detecting an anomaly of one of said code receiving means, said engine controlling means and said signal transmitting means; and

means for allowing start of the engine without receiving said engine start permission signal if said anomaly is detected.

2. An anti-theft protection system as claimed in claim 1, wherein

said start allowing means are operative when said engine start permission signal is received and that a subsequent anomaly of said one is detected.

3. An anti-theft protection system as claimed in claim 2, wherein said start allowing means are operative when said engine start permission signal is received and that a new engine start permission signal fails to be received.

4. An anti-theft protection system as claimed in claim 3, wherein said start allowing means comprise:

means for setting a flag if said engine start permission signal is received when the key is operated to an ignition turn-on position

said start allowing means being operative when said engine start permission signal fails to be received while said flag is set.

5. An anti-theft protection system as claimed in claim 4, wherein said start allowing means comprise:

means for resetting said flag if said anomaly fails to be detected when the key is operated to an ignition turn-off position,

said start allowing means being operative only when said new engine start permission signal is received while said flag is reset.

6. An anti-theft protection system as claimed in claim 5, wherein said flag is stored in a nonvolatile memory.

7. An anti-theft protection system as claimed in claim 1, wherein said signal transmitting means comprise:

means for determining whether said code as received coincides with said code as registered when the key is operated to an ignition turn-on position.

8. An anti-theft protection system as claimed in claim 1, wherein said anomaly detecting means detect said anomaly when a code transmitted from said engine controlling means to said signal transmitting means fails to coincide with a code returned from said signal transmitting means to controlling means.

9. An anti-theft protection system as claimed in claim 8, wherein said engine controlling means transmit to said signal transmitting means a new code corresponding to said engine start permission signal when the key is operated to said ignition turn-off position.

said signal transmitting means returning said new code to said engine controlling means,

said anomaly detecting means determining whether said new code transmitted from said engine controlling means to said signal transmitting means coincides with a new code returned from said signal transmitting means to said engine controlling means,

said anomaly detecting means detecting said anomaly when said new code transmitted from said engine controlling means to said signal transmitting means fails to coincide with said new code returned from said signal transmitting means to said engine controlling means.

10. An anti-theft protection system as claimed in claim 1, wherein said engine controlling means comprise:

means for determining whether a speed of the motor vehicle is greater than a predetermined speed;

means for determining whether a start operation of the engine is made by a key over a predetermined number, and

means for prohibiting start of the engine during a predetermined period of time, said start prohibiting means being operative when said speed is greater than said predetermined speed and that said start operation is carried out over said predetermined number.

11. An anti-theft protection system as claimed in claim 10, wherein said engine controlling means comprise:

means for stopping a collation of said code as received with said code as registered during said predetermined period of time, said collation stopping means being operative when said speed is greater than said predetermined speed and that said start operation is carried out over said predetermined number.

12. An anti-theft protection system as claimed in claim 11, wherein said engine controlling means comprise:

means for determining whether a noncoincidence of said code as received with said code as registered occurs over a predetermined number,

said collation stopping means being operative when said noncoincidence occurs over said predetermined number,

said start prohibiting means being operative when said noncoincidence occurs over said predetermined number.

13. An anti-theft protection system as claimed in claim 12, wherein said engine controlling means comprise:

means for resetting a count number of start operation of the engine and that of noncoincidence of said code to zero, and reopening said collation of said code after a lapse of said predetermined period of time.

14. An anti-theft protection system as claimed in claim 10, wherein said speed determining means include a speed detector.

15. An anti-theft protection system as claimed in claim 10, wherein said start operation determining means include a switch.

16. An anti-theft protection system as claimed in claim 1, wherein said engine controlling means comprise:

means for storing and engine start permission signal in a nonvolatile way.

17. An anti-theft protection system as claimed in claim 16, wherein said engine controlling means comprise:

means for detecting a stop operation of the engine made by the key; and

means for erasing said engine start permission signal as stored, said engine start permission signal erasing means being operative when said stop operation is detected.

18. An anti-theft protection system as claimed in claim 17, further comprising:

a connector arranged to connect a battery and said engine controlling means; and

means for detecting whether said connector ensures a connection between said battery and said engine controlling means.

19. An anti-theft protection system as claimed in claim 18, wherein said connector detecting means include terminals and a microcomputer.

20. An anti-theft protection system as claimed in claim 18, wherein said engine controlling means comprise:

means for storing a disconnection flag when said connector fails to ensure said connection,

said engine start permission signal erasing means being operative when said connector ensures said connection and that said disconnection flag is stored.

21. An anti-theft protection system as claimed in claim 1, further comprising:

means for putting the motor vehicle of one of a locked and alerted state and an unlocked and unalerted state at least on condition that said code as received coincides with said code as registered;

means for ensuring, in said locked and alerted state, a predetermined alarm action even when the motor vehicle is unlocked with the key; and

means for stopping said predetermined alarm action when said code as received coincides with said code as registered.

22. An anti-theft protection system as claimed in claim 21, wherein said predetermined alarm action ensuring means

ensuring said predetermined alarm action when detecting one of opening of a door, a trunk and a hood, releasing of a lock, and removal of said key cylinder.

23. An anti-theft protection system as claimed in claim 21, wherein said predetermined alarm action includes a visual alarm.

24. An anti-theft protection system as claimed in claim 23, wherein said predetermined alarm action includes an auditory alarm.

25. An anti-theft protection system as claimed in claim 1, wherein said signal transmitting means include a key cylinder.

26. An anti-theft protection system as claimed in claim 1, wherein said code receiving means include a transmitter-receiver.

27. An anti-theft protection system as claimed in claim 1, wherein said signal transmitting means include an immobilizer unit.

28. A method of protecting a motor vehicle from a theft, the motor vehicle having an engine, a key with a transponder, a transmitter-receiver, an engine control unit and an immobilizer unit, the method comprising the steps of: receiving a code of the key transmitted from the transponder;

transmitting an engine start permission signal to the engine control unit when said code as received coincides with a code as registered;

detecting an anomaly of one of the transmitter-receiver, the engine control unit and the immobilizer unit; and allowing start of the engine without receiving said engine start permission signal if said anomaly is detected.

29. A method as claimed in claim 28,

wherein said start allowing step is carried out when said engine start permission signal is received and that a subsequent anomaly of said one is detected.

30. A method as claimed in claim 29, wherein said start allowing step is carried out when said engine start permission signal is received and that a new engine start permission signal fails to be received.

31. A method as claimed in claim 29, wherein said anomaly detecting step is carried out to detect said anomaly when a code transmitted from the engine control unit to the immobilizer unit fails to coincide with a code returned from the immobilizer unit to the engine control unit.

32. A method as claimed in claim 31, further comprising the steps of:

transmitting from the engine control unit to the immobilizer unit a new code corresponding to said engine start permission signal when the key is operated to said ignition turn-off position;

returning said new code from the immobilizer unit to the engine control unit;

determining whether said new code transmitted from the engine control unit to the immobilizer unit coincides with a new code returned from the immobilizer unit to the engine control unit; and

detecting said anomaly when said new code transmitted from the engine control unit to the immobilizer unit fails to coincide with said new code returned from the immobilizer unit to the engine control unit.

33. A method as claimed in claim 28, further comprising the step of:

determining whether said code as received coincides with said code as registered when the key is operated to an ignition turn-on position.

34. A method as claimed in claim 33, further comprising the step of:

setting a flag if said engine start permission signal is received when the key is operated to said ignition turn-on position,

said start allowing step being carried out when said engine start permission signal fails to be received while said flag is set.

35. A method as claimed in claim 34, further comprising the step of:

resetting said flag if said anomaly fails to be detected when the key is operated to an ignition turn-off position,

said start allowing step being carried out only when said new engine start permission signal is received while said flag is reset.

36. A method as claimed in claim 35, wherein said flag is stored in a nonvolatile memory.

37. A method as claimed in claim 28, further comprising the steps of:

determining whether a speed of the motor vehicle is greater than a predetermined speed;

determining whether a start operation of the engine is made by the key over a predetermined number; and

prohibiting start of the engine during a predetermined period of time, said start prohibiting step being carried out when said speed is greater than said predetermined speed and that said start operation is carried out over said predetermined number.

38. A method as claimed in claim 37, further comprising the steps of:

stopping a collation of said code as received with said code as registered during said predetermined period of time, said collation stopping step being carried out when said speed is greater than said predetermined speed and that said start operation is carried out over said predetermined number.

39. A method as claimed in claim 38, further comprising the step of:

determining whether a noncoincidence of said code as received with said code as registered occurs over a predetermined number,

said collation stopping step being carried out when said noncoincidence occurs over said predetermined number.

40. A method as claimed in claim 39, further comprising the steps of:

resetting a count number of start operation of the engine and that of noncoincidence of said code to zero; and

reopening said collation of said code after a lapse of said predetermined period of time.

41. A method as claimed in claim 37, wherein said speed determining step is carried out with a speed detector.

42. A method as claimed in claim 37, wherein said start operation determining step is carried out with a switch.

43. A method as claimed in claim 28, further comprising the step of:

storing said engine start permission signal in a nonvolatile way.

44. A method as claimed in claim 43, further comprising the steps of:

detecting a stop operation of the engine made by the key; and

erasing said engine start permission signal as stored, said engine start permission signal erasing step being carried out when said stop operation is detected.

45. A method as claimed in claim 44, further comprising the steps of:

detecting whether a connector ensures a connection between a battery and the engine control unit; and storing a disconnection flag when said connector fails to ensure said connection,

said engine start permission signal erasing step being carried out when said connector ensures said connection and that said disconnection flag is stored.

46. A method as claimed in claim 45, wherein said connector detecting step is carried out with terminals and a microcomputer.

47. A method as claimed in claim 28, further comprising the steps of:

putting the motor vehicle in one of a locked and alerted state and an unlocked and unalerted state at least on condition that said code as received coincides with said code as registered;

ensuring, in said locked and alerted state, a predetermined alarm action even when the motor vehicle is unlocked with the key; and

stopping said predetermined alarm action when said code as received coincides with said code as registered.

48. A method as claimed in claim 47, wherein said predetermined alarm action ensuring step is carried out when detecting one of opening of a door, a trunk and a hood, releasing of a lock, and removal of a key cylinder.

49. A method as claimed in claim 48, wherein said predetermined alarm action includes a visual alarm.

50. A method as claimed in claim 49, wherein said predetermined alarm action includes an auditory alarm.

\* \* \* \* \*



US006285948B1

(12) **United States Patent**  
Takagi et al.

(10) Patent No.: **US 6,285,948 B1**  
(45) Date of Patent: **Sep. 4, 2001**

(54) **CONTROL APPARATUS AND METHOD  
HAVING PROGRAM REWRITING  
FUNCTION**

(75) Inventors: Noboru Takagi, Obu; Hajime  
Nomura, Okazaki, both of (JP)

(73) Assignee: Denso Corporation, Kariya (JP)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/543,897

(22) Filed: Apr. 6, 2000

(30) **Foreign Application Priority Data**

May 26, 1999 (JP) ..... 11-146646

(51) Int. Cl.<sup>7</sup> ..... G06F 15/02; B60R 25/10

(52) U.S. Cl. .... 701/115; 307/10.5; 340/5.23

(58) Field of Search ..... 701/101, 102,  
701/103, 114, 115; 307/10.1, 10.3, 10.4,  
10.5; 340/5.2, 5.23, 5.26, 5.72, 5.61, 5.64

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

5,610,574 \* 3/1997 Mutoh et al. .... 307/10.5  
5,763,958 \* 6/1998 Yamamoto et al. .... 307/10.5

5,769,051 \* 6/1998 Bayron et al. .... 701/115  
5,802,485 \* 9/1998 Koelle et al. .... 701/115  
5,803,043 \* 9/1998 Bayron et al. .... 701/115  
5,806,015 \* 9/1998 Kimoto ..... 701/115  
5,828,977 10/1998 Hayashi et al. .... 701/115  
5,896,095 \* 4/1999 Hill et al. .... 340/5.2  
6,163,271 \* 12/2000 Yoshizawa et al. .... 340/5.26  
6,194,991 \* 2/2001 Barrs et al. .... 340/5.72

**FOREIGN PATENT DOCUMENTS**

0 835 790 A2 4/1998 (EP) .  
09-128229 5/1997 (JP) .

\* cited by examiner

Primary Examiner—Willis R. Wolfe

(74) Attorney, Agent, or Firm—Nixon & Vanderhye P.C.

(57) **ABSTRACT**

In an engine control apparatus, a control program is stored in a non-volatile rewritable memory such as EEPROM. The control program is rewritten by a rewriting tool. Specifically, a key identification code is retrieved from a vehicle key, and compared with a key reference code stored in the memory. If the compared codes are the same, a program identification code is retrieved from the rewriting tool, and compared with a program reference code stored in the memory. If the compared codes are the same, a new control program is transmitted from the rewriting tool to the memory to rewrite the control program with the new control program.

26 Claims, 5 Drawing Sheets

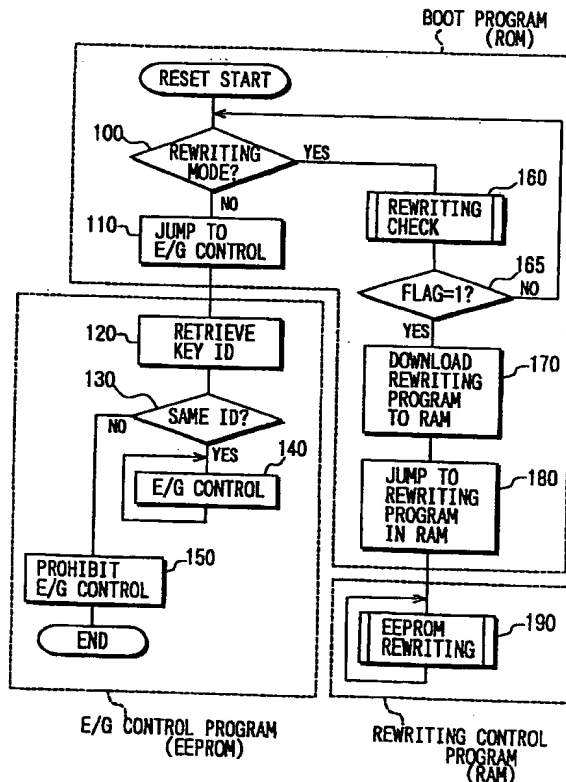


FIG. 1

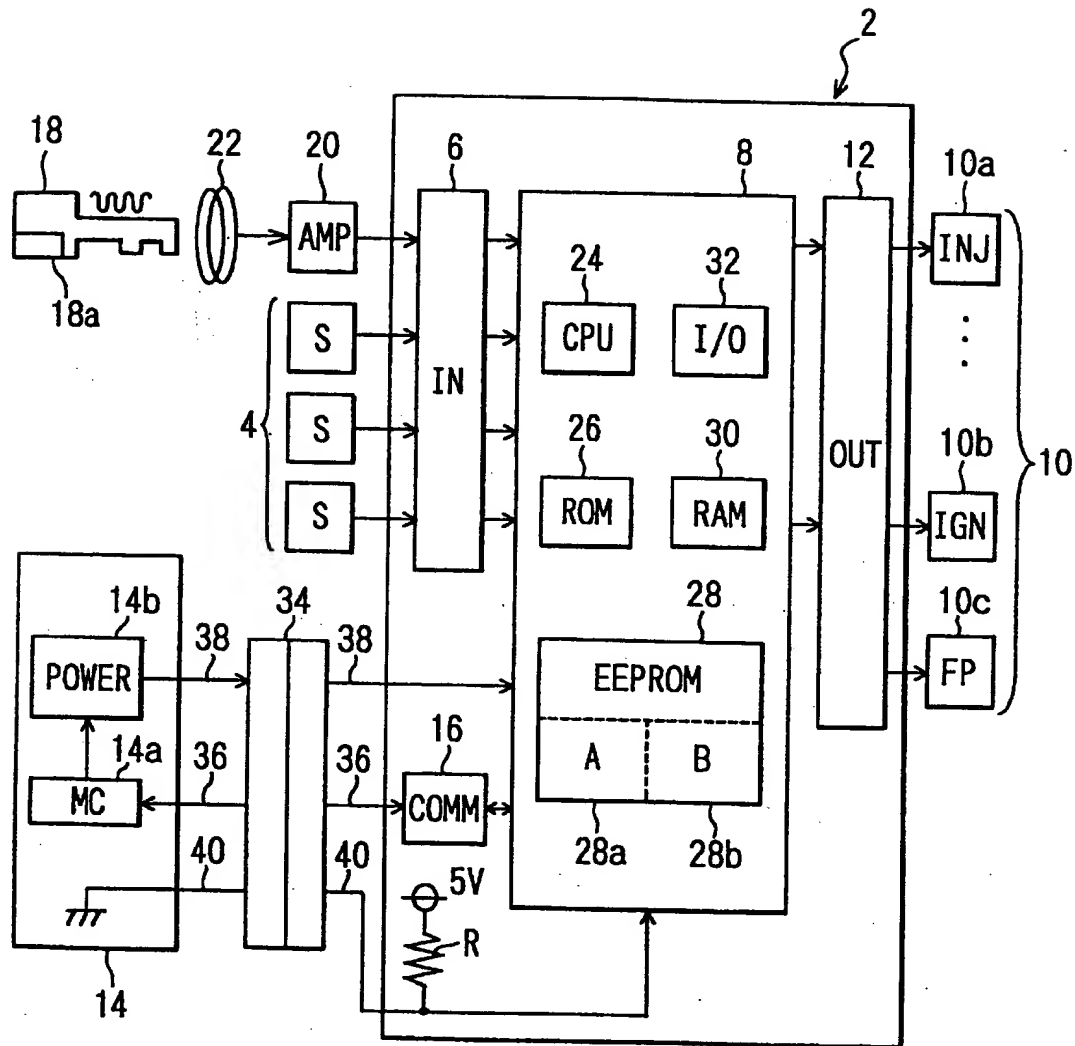


FIG. 2

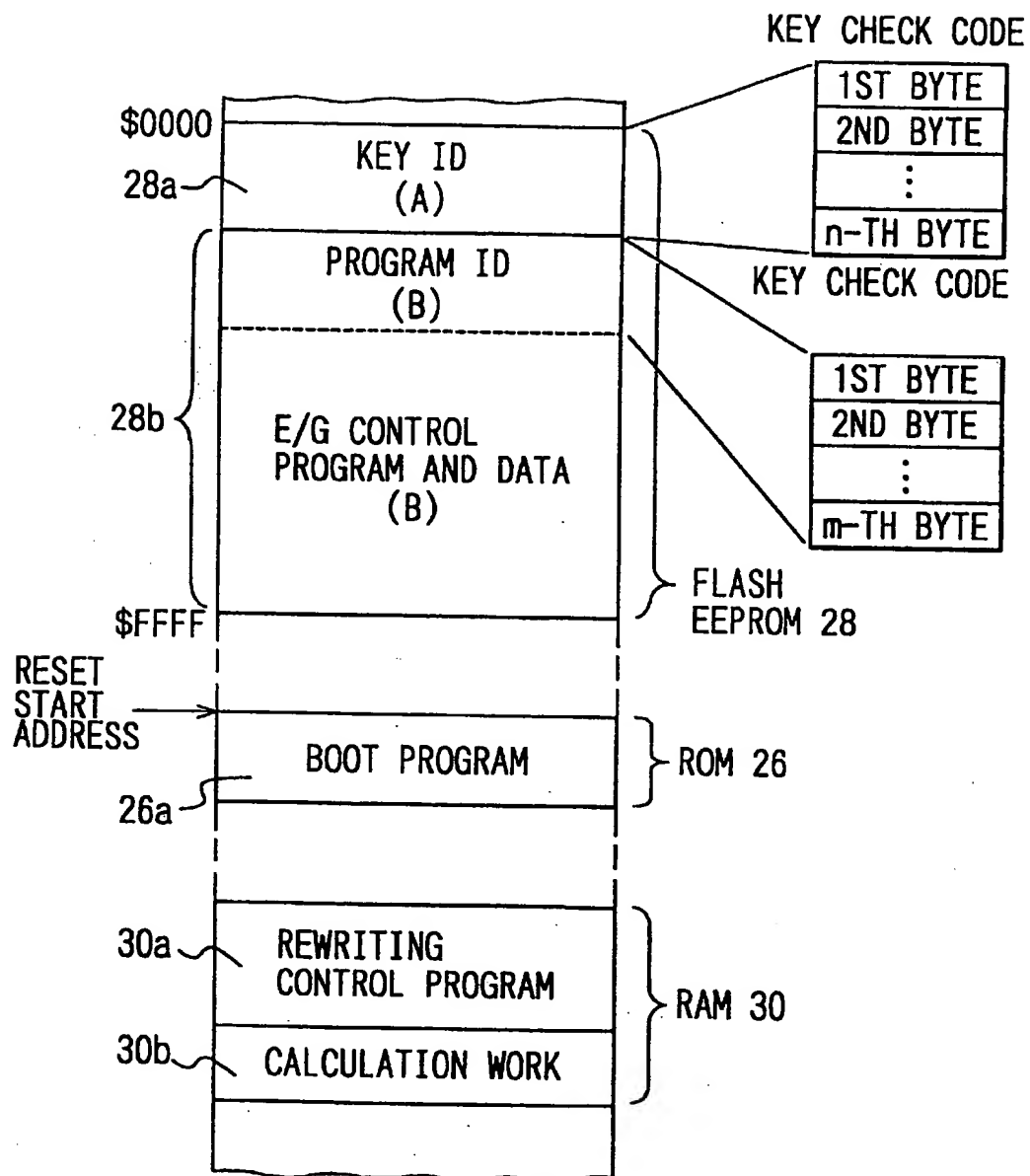
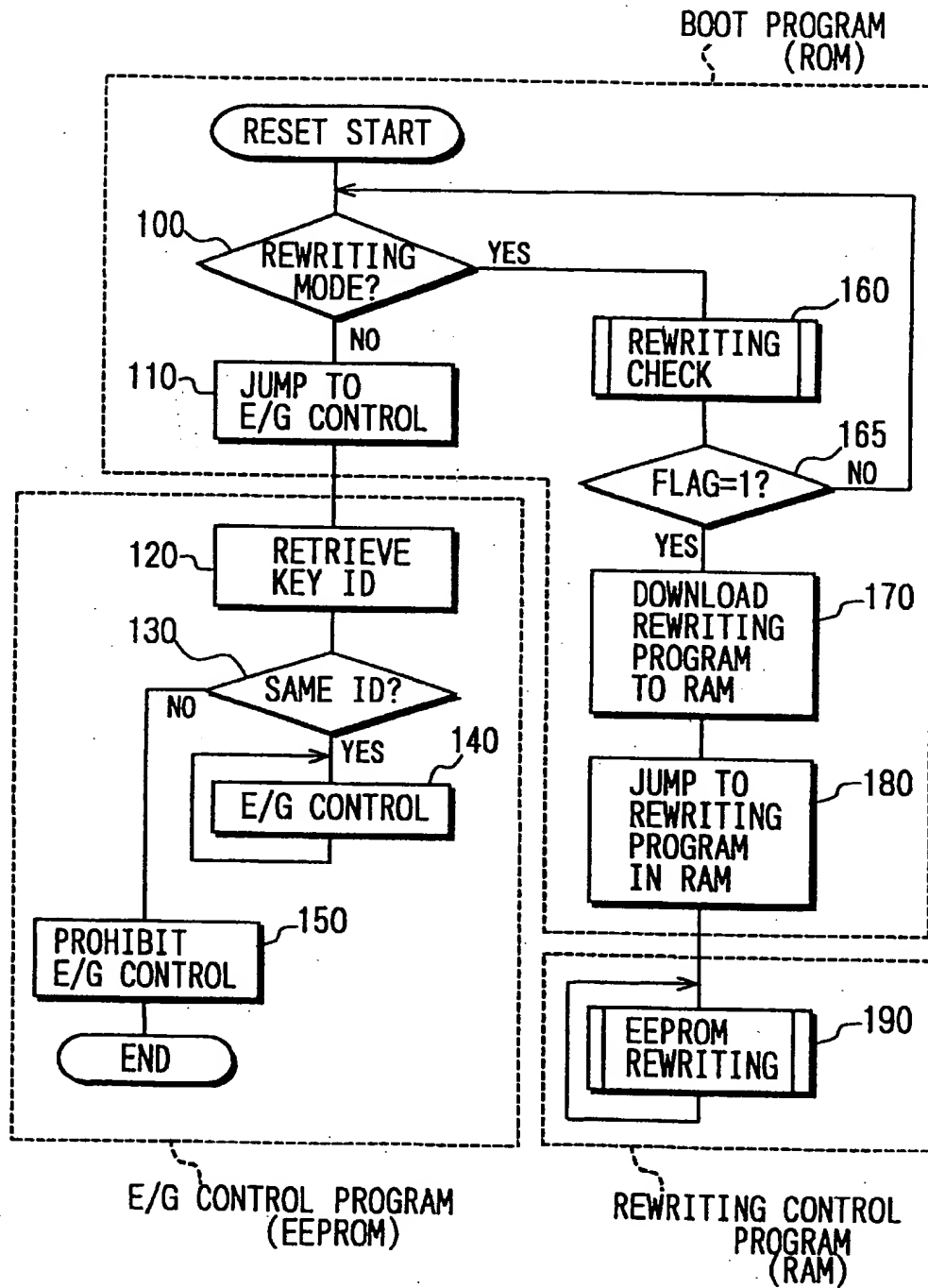




FIG. 3



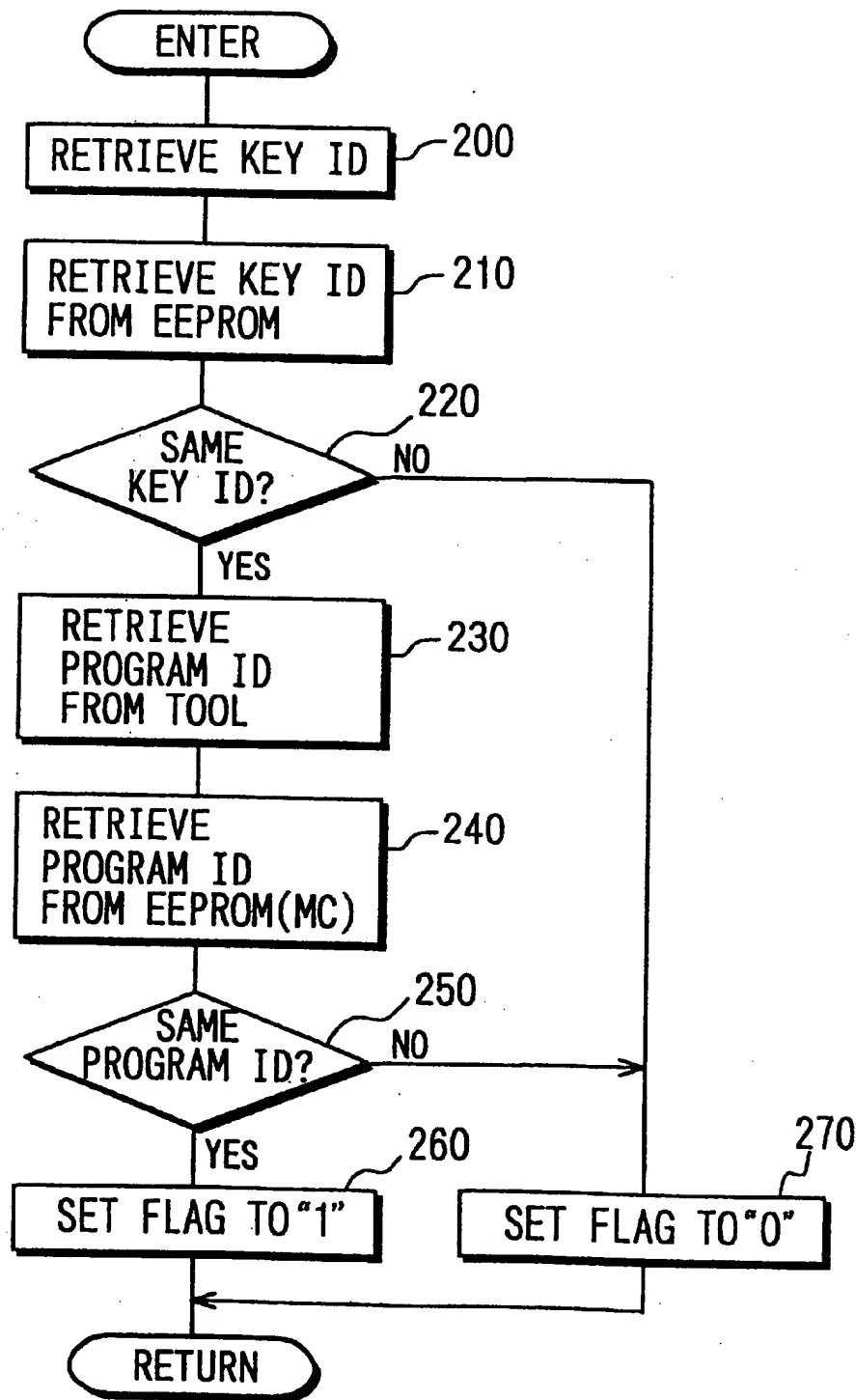
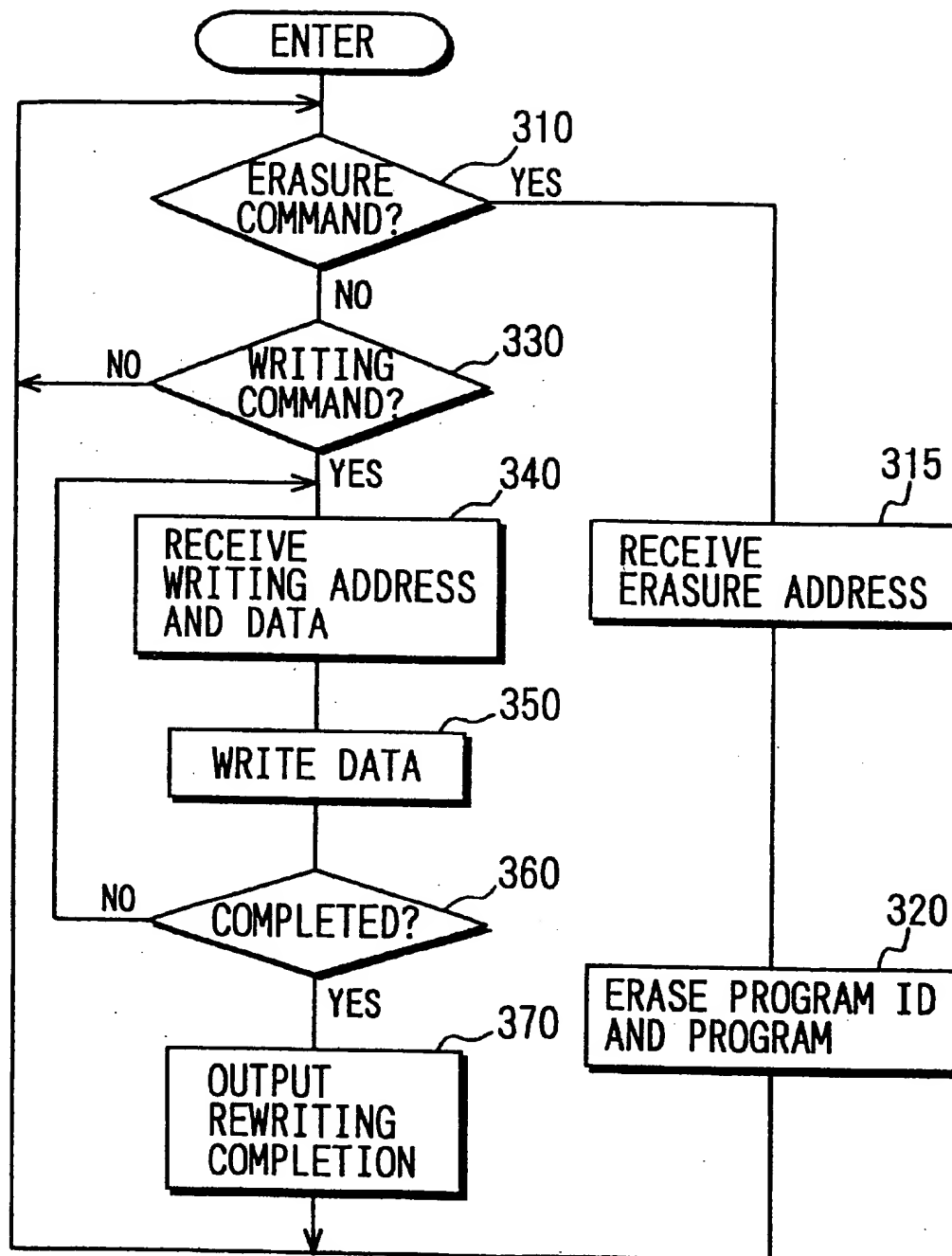
**FIG. 4**

FIG. 5



1

# CONTROL APPARATUS AND METHOD HAVING PROGRAM REWRITING FUNCTION

## CROSS REFERENCE TO RELATED APPLICATION

This application relates to and incorporates herein by reference Japanese Patent Application No. 11-146646 filed on May 26, 1999.

## BACKGROUND OF THE INVENTION

The present invention relates to electronic control apparatuses and methods, and more particularly to a program rewriting control and devices therefor which disables unauthorized rewriting of programs.

Many electronic control apparatuses are proposed for preventing intrusion into automotive vehicles and burglary of the same. In some apparatuses, an identification code (ID) of a key which a vehicle user uses is compared with a key ID which is stored in a non-volatile electrically erasable programmable read-only memory (EEPROM) of an electronic control unit (ECU) for engine control. Engine operations such as fuel injection and ignition are prohibited, if the compared key IDs do not agree or coincide.

It is a recent trend to design ECUs to be capable of rewriting or updating engine control programs stored in respective EEPROMs by using program rewriting tools. Thus, any defects in the control program of the ECU can be rectified without entirely replacing the ECU with a new one.

The program rewriting tool may be used to illegally rewrite the control program. That is, it may be used to rewrite control programs having an anti-burglary function (key ID check program) to control programs having no anti-burglary function by erasing the key ID check program. Thus, it is likely that vehicles will be intruded and stolen by using a key which does not have the same ID as stored in the EEPROM.

## SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a program rewriting control and devices therefor for preventing unauthorized intrusion and burglary.

According to the present invention, an electronic control unit has a non-volatile rewritable memory storing a program therein. An external rewriting device is connected to the electronic control unit when the program is to be rewritten. A first code such as a key identification code is transmitted from a transponder to the control unit. The control unit checks for an agreement between the first code and a second code stored in the control unit for attestation. A third code such as a program identification code is transmitted from the rewriting tool to the control unit. The control unit checks for an agreement between the third code and a fourth code stored in the electronic control unit for attestation. A new program is transmitted from the rewriting tool to the electronic control unit, preferably when check results are in predetermined relations, respectively. The stored program in the rewritable memory is rewritten by the transmitted new program.

## BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of the present invention will become more apparent from the following detailed description made with reference to the accompanying drawings. In the drawings:

2

FIG. 1 is a block diagram showing an electronic control apparatus for engines having a program rewriting control function according to an embodiment of the present invention;

FIG. 2 is a schematic diagram showing a construction of a memory used in the embodiment shown in FIG. 1;

FIG. 3 is a flow diagram showing an entire program executed in an ECU used in the embodiment shown in FIG. 1;

FIG. 4 is a flow diagram showing rewriting check processing which is a part of the program shown in FIG. 3; and

FIG. 5 is a flow diagram showing EEPROM rewriting processing which is a part of the program shown in FIG. 3.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention will be described in further detail with reference to its embodiment. The present invention is applied to an electronic control apparatus for automotive vehicle engines in the following embodiment.

Referring first to FIG. 1, an electronic control apparatus is comprised of an electronic control unit (ECU) 2 for engines, sensors 4, and actuators 10 such as injectors 10a, an igniter 10b and a fuel pump 10c. The ECU 2 includes an input circuit 6 for wave-shaping sensor signals from the sensors 4, a microcomputer 8 for calculating optimum engine control amounts such as fuel injection amount, ignition timing and fuel pressure, and an output circuit 12 for driving the actuators 10 based on the calculated control amounts. The ECU 2 also includes a communication circuit 16, which executes communications between a program rewriting tool 14 and the microcomputer 8 when an engine control program is to be rewritten or updated.

A vehicle key 18 is an electronic-type key which is provided with a transponder 18a. The transponder 18a is provided therein with a n-bit key identification code (ID) exclusive thereto. An antenna 22 is connected to the input circuit 6 through an amplifier 20, so that the key ID may be applied to the microcomputer 8 therethrough. The transponder 18a is constructed to receive and store electric power in its capacitor upon reception of excitation signals from a vehicle side, when the key 18 is inserted into a key cylinder. Further, the transponder 18a is constructed to operate as a signal transmitter/receiver with the stored electric power.

The microcomputer 8 has a central processing unit (CPU) 24 which operates on stored programs, non-volatile read-only memory (ROM) 26 which stores the programs and data, non-volatile electrically erasable programmable read-only memory (EEPROM) 28 which stores programs and data, and a random access memory (RAM) 30 which stores the calculation results of the CPU 24 and the like. The microcomputer 8 further has an input/output circuit 32 which receives signals from the input circuit 6 and the communication circuit 16, and outputs control signals to the output circuit 12.

The EEPROM 28 stores in its A-storage area 28a a predetermined key ID exclusive to the ECU 2, and in its B-area a program ID and a program. The EEPROM 28 may be a flash type (erasable/rewritable) which is capable of erasing and rewriting a part of data once written.

The program rewriting tool 14 is used as an external device to the ECU 2. The rewriting tool 14 has a microcomputer 14a and a power circuit 14. The microcomputer 14a is programmed to execute serial communications with the microcomputer 8 so that the program and/or data stored

in the EEPROM 28 may be rewritten therethrough. The power circuit 14b is constructed to supply the microcomputer 8 with a high voltage (12 volts) required to rewrite the EEPROM 28.

The ECU 2 and the rewriting tool 14 are connected to each other through respective communication lines 36, power supply lines 38 and mode check lines 40 through an electrical connector 34. The electrical connector 34 normally separates the rewriting device 14 from the ECU 2, but connects them when rewriting the program and data of the EEPROM 28 is required. The microcomputer 8 of the ECU 2 and the microcomputer 14a of the rewriting tool 14 are enabled to execute serial communications therebetween through the communication lines 36. The microcomputer 8 of the ECU 2 is supplied with the required voltage (12 V) from the power circuit 14b of the rewriting tool 14 through the power supply lines 38 to rewrite the EEPROM 28.

The mode check line 40 is pulled up to a positive voltage (5 V) in the ECU 2 by a resistor R, and is connected to ground (0 V) in the rewriting tool 14. When the rewriting device 14 is connected to the ECU 2 through the connector 34, the mode check line 40 in the ECU 2 is changed to low level (0 V) from its normal high level (5 V). The microcomputer 8 thus determines with this low level that the rewriting tool 14 is connected to the ECU 2.

The EEPROM 28 has two storage areas, that is, the A-area 28a and B-area 28b, as shown in FIG. 2. The A-area 28a stores therein a key identification code (key ID) having "n" bytes (for instance 8 bytes) which varies from ECU to ECU (vehicle to vehicle). The B-area 28b stores therein a program and data for engine controls. The B-area 28b specifically stores at the head address thereof preceding program and data addresses a program identification code (program ID) having "m" bytes (for instance 4 bytes) indicative of the engine control program. The key ID is for checking whether the key 18 is an authorized one. The program ID is for checking the vehicle model, destination and program version.

The ROM 26 has a storage area 26a in which a boot program is stored. The boot program is executed immediately after a reset operation. The RAM 30 has two storage areas, that is, EEPROM rewriting control program storage area 30a and operation work area 30b. The storage area 30a is used to store therein an EEPROM rewriting control program transmitted from the rewriting tool 14. The work area 30b is used in the course of execution of the transmitted rewriting control program.

The EEPROM 28, ROM 26 and RAM 30 store in each address thereof 8-bit data. The A-area 28a and B-area 28b of the EEPROM 28 are set to 64K bytes, from address \$0000 to address \$FFFF.

The microcomputer 8 is programmed to initiate the boot program set as the reset start address as shown in FIG. 2 immediately after the reset operation. It is also programmed to call the engine control program by the boot program and execute the same, when the rewriting tool 14 is not connected.

When the microcomputer 8 determines that the rewriting tool 14 is connected at the time of initiation of the boot program, it stores in the rewriting program storage area 30a of the RAM 30 the rewriting control program transmitted from the rewriting tool 14 through the communication lines 38. Then, it initiates the stored rewriting control program to rewrite or update the existing program ID and program stored in the EEPROM 28 with the new program ID and program transmitted from the rewriting tool 14.

This operation of the microcomputer 8, particularly CPU 24, is described in detail with reference to FIGS. 3 to 5.

The CPU 24 is reset to start its operation when the ECU 2 is powered on with electric power. The CPU 24 first executes the boot program stored in the ROM 26.

Specifically, the CPU 24 first checks at step 100 whether the mode check line 40 is at the low level indicating the EEPROM rewriting mode. If it is not the rewriting mode, the CPU 24 determines that the rewriting device 14 is not connected. The processing then jumps at step 110 to the engine control program stored in the EEPROM 28.

The CPU 24 then retrieves or reads out the key ID indicative of the key 18. Specifically, the CPU 24 drives the amplifier circuit 20 to transmit the excitation signal from the antenna 22 to the transponder 18a of the key 18. The CPU 24 terminates the excitation operation after a predetermined time period (for instance 50 ms). The transponder 18a is thus energized to operate. The CPU 24 then drives the amplifier 20 to transmit a request signal from the antenna 22 to the transponder 18a. The transponder 18a in response transmits a key identification code (key ID) signal specific to the key 18 to the antenna 22. Thus, the CPU 24 determines the key ID from the received key ID signal.

The CPU 24 then checks at step 130 whether the retrieved key ID coincides with (same as) the key ID stored in the EEPROM 28. In this checking step, all numerical value of byte data of the key ID (FIG. 2) are checked for agreement. The CPU 24 executes steps 140 and 150, if all byte data are the same (key 18 is the authorized one) and any one of byte data is different (key 18 is not the authorized one), respectively.

At step 140, the CPU 24 repeatedly executes the engine control processing. Specifically, the CPU 24 calculates the optimum fuel injection amount, ignition timing and the like based on the engine operating conditions detected by sensors 4 and the engine control data stored in the EEPROM 28. It produces the control signals to drive the actuators 10 through the output circuit 12 based on the calculation results. At step 150, however, the CPU 24 prohibits the engine control and ends this routine. That is, it disables the operations of the actuators 10.

If it is the rewriting mode (YES at step 100), on the other hand, the CPU 24 executes a rewriting processing at step 160. In this rewriting check processing, the CPU 24 checks whether the key ID retrieved from the key 18 and the key ID stored in the EEPROM 28 are the same, and further whether the program ID retrieved stored in the rewriting tool and the program ID stored in the EEPROM 28 are the same.

This rewriting check processing at step 160 is described in further detail with reference to FIG. 4.

The CPU 24 first retrieves the key ID from the transponder 18 at step 200 in the same manner as in step 120, and retrieves the key ID from the EEPROM 28. The CPU 24 then checks at step 220 whether the two retrieved key IDs are the same. The CPU executes steps 230 and 270 if the key IDs are the same (YES) and different (NO), respectively.

At step 270, the CPU 24 sets a rewriting flag to "0" and ends this sub-routine. The rewriting flag "0" indicates use of unauthorized key and is set to "0" each time the CPU 24 is initialized. At step 230, however, the CPU 24 retrieves the program ID stored in the rewriting tool 14. The CPU 24 then retrieves the program ID stored in the EEPROM 28 of the microcomputer 8 at step 240, and checks at step 250 whether the two retrieved program IDs are the same.

In this program ID checking processing, the two IDs are compared byte by byte with respect to the vehicle model and

5

the destination. The CPU 24 provisionally determines YES and NO, if all the compared data byte are the same and if any compared data byte is different, respectively. The CPU 24 further checks whether the version data in the program ID received from the rewriting tool 14 are the same as or newer than that stored in the EEPROM 28. The CPU 24 finally determines YES, only when the vehicle model data and the destination are the same and the version data are the same or new.

The CPU 24 sets at step 260 the rewriting flag to "1" in response to the check result YES of step 250 indicating that the program ID of the rewriting tool 14 is the same as that stored in the EEPROM 28. However, it sets the flag to "0" at step 270 in response to the check result NO of step 250. Thus, the flag "1" indicates that the rewriting program of the rewriting tool 14 is an acceptable or appropriate one.

After the above rewriting check processing at step 160, the CPU 24 executes step 165 to check whether the rewriting flag is "1", that is, whether the control program and data rewriting should be executed. The CPU 24 executes step 170 or step 100, if the check result is YES and NO, respectively. At step 170, the CPU 24 downloads the rewriting program from the rewriting tool 14 into the RAM 30 of the micro-computer 8 through the communication lines 38. The CPU 24 then executes step 180 to initiate the rewriting program stored in the RAM 30.

The CPU 24 then executes the control program and data rewriting processing at step 190 based on the initiated rewriting program. That is, the CPU 24 rewrites or updates the control program and data for the engine control stored in the EEPROM 28 with new control programs and data which is sent from the rewriting tool 14.

The rewriting processing at step 190 is shown in detail in FIG. 5. Specifically, the CPU 24 first checks at step 310 whether an erasure command has been received from the rewriting tool 14. If it has been received (YES), the CPU 24 receives at step 315 erasure addresses, that is, addresses of the program ID and the control program stored in the EEPROM 28 which are to be erased. The CPU 24 then erases at step 320 the contents in the designated erasure addresses, that is, the program ID and the control program.

If the erasure command has not been received (NO at step 310), the CPU 24 checks at step 330 whether a writing command has been received from the rewriting tool 14. If it has been received (YES), the CPU 24 receives at step 340 the writing addresses and new data or contents from the rewriting tool 14. The new contents includes the program ID and new program to be rewritten. The CPU 24 then writes at step 350 the received new data over the previous one stored in the designated addresses of the EEPROM 28.

The CPU 24 then checks at step 360 whether the new data have all been rewritten into the EEPROM 28, that is, whether the rewriting operation has been completed. The CPU 24 repeats the above steps 340 to 360 until all new data have been rewritten. If the rewriting operation has been completed (YES), the CPU 24 outputs at step 370 a rewriting completion signal to the rewriting tool 14 through the communication lines 36. The rewriting tool 14 may preferably be constructed to display a rewriting completion message on its display unit.

According to the present embodiment, the rewriting is enabled only when the key ID agrees to the stored one in the ECU 2. Thus, the rewriting operation is disabled when the key 18 is an unauthorized one, improving the anti-burglary function. As long as the key 18 is an authorized one, the control program and data of the ECU 2 can be rewritten to

6

rectify any detects in the control program and data at maintenance shops, etc., while maintaining the ECU 2 as mounted in the vehicle.

Further, the rewriting is enabled only when the program ID of the rewriting tool 14 agrees to the stored one in the ECU 2 in addition to the agreement of the key ID. Thus, the ECU 2 is protected from being illegally changed to have improper control program and data, thus improving further the anti-burglary function.

In addition, the key ID is stored in the EEPROM 28 and rewritable. The key ID can be changed to a new one, immediately after the key 18 is stolen. As a result, the ECU 2 can be protected from any unauthorized rewriting which may be tried by using the stolen key 18.

The present invention may also be implemented as follows.

In this embodiment, a ciphered function data is used as an attestation data in place of the key ID used in the above embodiment. Therefore, the transponder 18a of the key 18 is constructed to store the function data  $Ft(X)$ , and the EEPROM 28 is constructed to store the same function data  $Ft(X)$ . For instance, the function  $Ft(X)$  may be defined as follows by using addition, subtraction, multiplication and/or division.

$$Ft(X) = (X^2 + 2)/5 + X/2 + (X - 1)/2 +$$

In operation, the CPU 24 drives the amplifier circuit 20 to transmit the excitation signal from the antenna 22, so that the transponder 18a is energized. The CPU 24 then outputs an interrogatory data X to the amplifier circuit 20. This data X is a digital data which is a combination of "1" and "0". The amplifier circuit 20 converts or modulates each bit of the interrogatory data into corresponding signal frequency F0 or F2 and transmit it as the request signal from the antenna 22 to the key 18.

The transponder 18a calculates an answer data Yt from the function data  $Ft(X)$  using the interrogatory data X as a variable. It then transmits a reply signal having frequencies F0 and F1 in correspondence with the calculated data Yt which is also a digital data (combination of "1" and "0"). The amplifier circuit 20 receives this reply signal through the antenna 22, and converts or demodulates it into a corresponding digital data.

The CPU 24 calculates its answer data Ye from a function data Fe(X) stored in the EEPROM 28 using the interrogatory data X which is also used to transmit the request signal to the key 18. The CPU 24 then checks whether the key 18 is an authorized one by comparing the two calculated data Yt and Ye. This embodiment will provide a higher anti-burglary function owing to the use of ciphered function data.

The present invention should not be limited to the embodiments described above, but may further be modified as follows.

For instance, the key ID may be stored in the ROM 26 in place of being stored in the EEPROM 28 so that it may not be changed. The program rewriting may be enabled by checking for an agreement between one of the key IDs or the program IDs. The key ID, control program and program ID may be stored in separate memories using a plurality of EEPROMs. The EEPROM may be replaced with other types of rewritable ROMs. The rewriting control program may be stored in a non-rewritable ROM in place of storing it in the rewriting tool 14 and downloading it into the RAM 30. The ECU may be for a vehicle brake control, transmission control, suspension control or the like. The transponder 18a may be provided separately from the key 18.

7

Further, an anti-burglary device may be provided separately from the ECU 2. That is, the anti-burglary device may be provided between the amplifier circuit 20 and the ECU 2. In this instance, the anti-burglary device is constructed to apply an engine-start enabling code to the ECU 2, after the agreement between the key 1ds is confirmed by the anti-burglary device. The ECU 2 stores in its EEPROM an engine-start enabling code. The ECU 2 checks for an agreement of the engine-start enabling codes received from the anti-burglary device and stored in the EEPROM 28.

Still further, in the case of using the ciphered function data, the key 18 may be determined as the authorized one as long as the calculation results  $Y_t$  and  $Y_e$  are in a predetermined relation.

In addition, the microcomputer 8 may be programmed to disable the rewriting operation when a vehicle engine is in the cranking condition. In this instance, the microcomputer 8 checks whether the engine is cranking, after step 165 shown in FIG. 3 determines YES (flag=1). The microcomputer 8 is allowed to execute the following step 170, only when it is confirmed that the engine is not in the cranking condition. The microcomputer 8 is programmed to disable the rewriting operation by just repeating a predetermined sequence of steps so that the rewriting process may be skipped, or to shut down a supply of power.

The rewriting control may also be applied to other devices than vehicle control, as long as a program in a memory such as micro chip, floppy disk, hard disk, optical disk and the like is to be rewritten.

What is claimed is:

1. An electronic control apparatus comprising:

a memory having a first storage area for storing an attestation data, and a second storage area for storing a control content required for controlling a control object and capable of rewriting the control content;  
input means for inputting a code data transmitted from an external device which allows an operation of the control object;

checking means for checking for an agreement between the transmitted code data and the stored attestation data; and

rewriting means for rewriting the control content in the second storage area in response to a check result of the checking means.

2. A program rewriting method for an electronic control unit comprising:

connecting a rewriting tool to the electronic control unit which stores a program therein;

transmitting a first code from a transponder to the electronic control unit;

checking for, within the electronic control unit, an agreement between the first code and a second code stored in the electronic control unit;

transmitting a third code from the rewriting tool to the electronic control unit;

checking for, within the electronic control unit, an agreement between the third code and a fourth code stored in the electronic control unit;

transmitting a new program from the rewriting tool to the electronic control unit, when check results of the checking steps are in predetermined relations, respectively; and

rewriting the stored program by the new program.

3. An electronic control apparatus comprising:

a first non-volatile memory storing an attestation reference data of a key;

8

a second non-volatile memory storing a control content required for controlling a control object, the second memory being capable of rewriting the control content in response to a predetermined operation of the key and an external rewriting command;

retrieving means for retrieving an attestation data of the key;

checking means for checking for an agreement between the retrieved attestation data and the stored reference data; and

disabling means for disabling rewriting of the control content stored in the second non-volatile memory, when a check result of the checking means indicates a disagreement between the retrieved attestation data and the stored reference data.

4. An electronic control apparatus of claim 3, wherein the control content includes at least one of a control program and a data used in execution of the control program.

5. An electronic control apparatus of claim 3, wherein the first non-volatile memory is a rewritable type capable of rewriting the stored reference data.

6. An electronic control apparatus of claim 3, wherein the first non-volatile memory is incapable of rewriting the stored reference data.

7. An electronic control apparatus of claim 3, further comprising:

a circuit for transmitting a request signal to a transponder associated with the key and receiving a response signal including the attestation data from the transponder.

8. An electronic control apparatus comprising:

a non-volatile memory storing a program and an attestation data of the stored program, and capable of rewriting the stored program;

retrieving means for retrieving from an external device an attestation data of a new program to be written over the stored program;

checking means for checking for an agreement between the retrieved attestation data of the new program and the stored identification data; and

disabling means for disabling rewriting of the new program into the non-volatile memory, when a check result of the checking means indicates a disagreement between the retrieved attestation data and the stored attestation data.

9. An electronic control apparatus of claim 8, wherein the attestation data is a predetermined identification data.

10. An electronic control apparatus of claim 8, wherein the attestation data is a predetermined ciphered function data.

11. An electronic control apparatus of claim 8, wherein: the non-volatile memory is for further storing a reference data;

the retrieving means is for further retrieving a key data from the key;

the checking means is for further checking for an agreement between the retrieved key data and the reference data; and

disabling means for further disabling rewriting of the new program into the non-volatile memory, when a check result of the checking means indicates a disagreement between the retrieved key data and the stored reference data.

12. An electronic control apparatus of claim 11, further comprising:

prohibiting means for prohibiting execution of the program stored in the non-volatile memory when the check

9

result of the checking means indicates the disagreement between the retrieved key data and the stored reference data.

13. An electronic control apparatus comprising:

a memory having a first storage area for storing an attestation data, and a second storage area for storing a control content required for controlling a control object and capable of rewriting the control content;

input means for inputting a code data transmitted from an external transponder;

checking means for checking for an agreement between the transmitted code data and the stored attestation data; and

rewriting means for rewriting the control content in the second storage area in response to a check result of the checking means.

14. An electronic control apparatus of claim 13, wherein the rewriting means is for disabling rewriting of the control content in the second storage area, when a check result of the checking means indicates a disagreement between the transmitted code data and the stored attestation data.

15. An electronic control apparatus of claim 13, wherein the rewriting means is for enabling rewriting of the control content in the second storage area, only when a check result of the checking means indicates the agreement between the transmitted code data and the stored attestation data.

16. An electronic control apparatus of claim 13, wherein the memory includes, as the first storage area, a non-volatile memory device capable of rewriting the stored attestation data.

17. An electronic control apparatus of claim 13, wherein the memory includes, as the first storage area, a non-volatile memory device incapable of rewriting the stored attestation data.

18. An electronic control apparatus of claim 13, wherein: the transmitted code data is stored in the transponder; the input means is for further transmitting a request signal to the transponder; and

the transponder is for transmitting the code data to the input means in response to the request signal.

10

19. An electronic control apparatus of claim 13, wherein a predetermined program sequence is repeated without rewriting, when a check result of the checking means indicates a disagreement between the transmitted code data and the stored attestation data.

20. An electronic control apparatus of claim 13, wherein a power supply is shut down, when a check result of the checking means indicates a disagreement between the transmitted code data and the stored attestation data.

21. An electronic control apparatus of claim 13, wherein the control content includes at least one of a control program and a data used in execution of the control program.

22. An electronic control apparatus of claim 21, wherein: the second storage area is for further storing the data used in execution of the control program as another code data;

the first storage area is for further storing program attestation data;

the checking means is for further checking an agreement between the another code data and the program attestation data; and

the rewriting means is for further disabling rewriting of the control program into the second storage area, when a check result of the checking means indicates a disagreement between the another code data and the program attestation data.

23. An electronic control apparatus of claim 22, wherein the another code data is a ciphered function data.

24. An electronic control apparatus of claim 13, wherein the control content is a control program for controlling an engine of a vehicle.

25. An electronic control apparatus of claim 24, wherein the transponder is integrated with a key for operating the engine.

26. An electronic control apparatus of claim 25, wherein the rewriting means is for further rewriting the control data when the key is inserted into a key cylinder and before the engine is operated.

\* \* \* \* \*





US006112152A

**United States Patent** [19][11] **Patent Number:** **6,112,152****Tuttle**[45] **Date of Patent:** **\*Aug. 29, 2000****[54] RFID SYSTEM IN COMMUNICATION WITH VEHICLE ON-BOARD COMPUTER****[75] Inventor:** John R. Tuttle, Boise, Id.**[73] Assignee:** Micron Technology, Inc., Boise, Id.**[\*] Notice:** This patent is subject to a terminal disclaimer.**[21] Appl. No.:** 09/378,435**[22] Filed:** Aug. 20, 1999**Related U.S. Application Data****[63]** Continuation of application No. 08/759,737, Dec. 6, 1996, Pat. No. 5,995,898.**[51] Int. Cl.<sup>7</sup>** ..... G08G 1/017; G07C 5/00; G06F 13/00; H04L 9/00**[52] U.S. Cl.** ..... 701/115; 701/101; 701/102; 701/114; 701/117; 340/348; 340/825.34**[58] Field of Search** ..... 701/102, 114, 701/101, 33, 115, 117; 340/438, 991, 933, 539, 825.34; 455/546**[56] References Cited****U.S. PATENT DOCUMENTS**

4,072,850	2/1978	McGlynn	701/35
4,075,632	2/1978	Baldwin et al.	343/6.8
4,107,689	8/1978	Jellinek	340/991
4,168,679	9/1979	Ikeura et al.	123/32
4,237,830	12/1980	Stivender	123/493

(List continued on next page.)

**FOREIGN PATENT DOCUMENTS**

0 456 425	5/1991	European Pat. Off. .
0 725 377	8/1996	European Pat. Off. .
2 647 930	6/1989	France .
3445668	12/1984	Germany .
2 169 173	7/1986	United Kingdom .
2277844	11/1994	United Kingdom .
WO 90/12365	10/1990	WIPO .
WO 91/18452	11/1991	WIPO .
WO 93/04353	3/1993	WIPO .
WO 94/07206	3/1994	WIPO .
WO 95/01607	1/1995	WIPO .
98/25248	6/1998	WIPO .

**OTHER PUBLICATIONS**

"Engine Air Control—Basis of a Vehicular Systems Control Hierarchy", Donald L. Stivender, Society of Automotive Engineers, Inc., 1978.

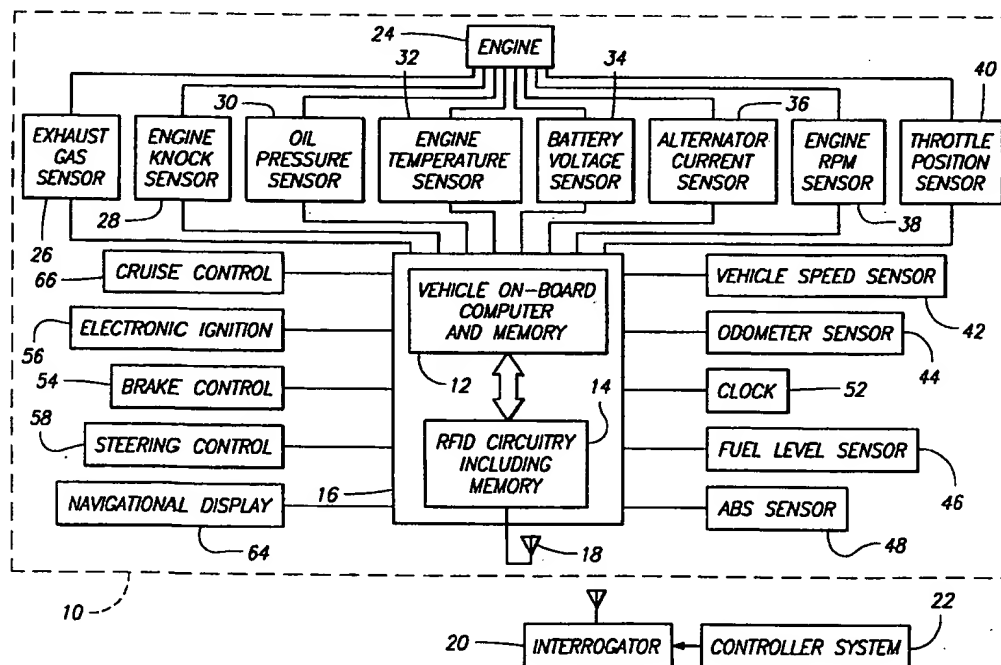
*Primary Examiner*—Henry C. Yuen

*Assistant Examiner*—Hieu T. Vo

*Attorney, Agent, or Firm*—Wells, St. John, Roberts, Gregory & Matkin, P.S.

**[57]****ABSTRACT**

A system comprising a vehicle on-board computer; and a wireless transponder device coupled to the vehicle on-board computer. The system performs a variety of functions because of its ability to transmit and receive data from other transponders which may be remote from the vehicle or located in the vehicle at a location spaced apart from the system. Remote transponders are spaced apart from the vehicle. The remote transponders can be positioned, for example, at a gas station, toll booth, service center, dealership, parking lot, or along a roadside.

**41 Claims, 4 Drawing Sheets**

## U.S. PATENT DOCUMENTS

4,335,695	6/1982	Phipps	123/478	5,586,034	12/1996	Takaba et al.	364/431.04
4,398,172	8/1983	Carroll et al.	340/38	5,598,898	2/1997	Mutoh et al.	180/287
4,497,057	1/1985	Kato et al.	371/29	5,606,306	2/1997	Mutoh et al.	340/426
4,524,745	6/1985	Tominari et al.	123/478	5,610,574	3/1997	Motoh et al.	340/426
4,551,803	11/1985	Hosaka et al.	701/115	5,619,412	4/1997	Hapka	701/112
4,552,116	11/1985	Kuroiwa et al.	123/489	5,621,380	4/1997	Mutoh et al.	340/426
4,714,925	12/1987	Bartlett	340/825.55	5,621,381	4/1997	Kawachi et al.	342/51
4,728,922	3/1988	Christen et al.	340/991	5,621,412	4/1997	Sharpe et al.	342/51
4,843,557	6/1989	Ina et al.	364/431.11	5,631,501	5/1997	Kubota et al.	307/10.5
4,853,850	8/1989	Krass, Jr. et al.	364/200	5,634,190	5/1997	Wiedman	455/13.1
4,875,391	10/1989	Leising et al.	74/866	5,635,693	6/1997	Benson et al.	340/825.54
4,878,050	10/1989	Kelley	340/825.06	5,649,296	7/1997	MacLellan et al.	455/38.2
4,908,792	3/1990	Przybyla et al.	364/900	5,660,246	8/1997	Kaman	180/287
4,926,182	5/1990	Ohta et al.	342/44	5,664,113	9/1997	Worger et al.	705/28
4,986,229	1/1991	Suzuki et al.	123/179	5,677,667	10/1997	Lesesky et al.	340/431
5,002,031	3/1991	Kako	123/486	5,686,920	11/1997	Hurta et al.	342/42
5,019,799	5/1991	Oshiage et al.	340/438	5,710,703	1/1998	Kirn et al.	364/424.034
5,054,569	10/1991	Scott et al.	340/825.54	5,712,899	1/1998	Pace, II	379/58
5,058,044	10/1991	Stewart et al.	340/825.54	5,717,830	2/1998	Sigler et al.	455/426
5,091,858	2/1992	Paielli	364/431.12	5,719,550	2/1998	Bloch et al.	340/426
5,113,427	5/1992	Ryoichi et al.	340/825.44	5,721,678	2/1998	Widl	364/424.04
5,150,609	9/1992	Ebner et al.	73/117.3	5,724,426	3/1998	Rosenow et al.	380/25
5,172,321	12/1992	Ghaem et al.	364/444.2	5,726,630	3/1998	Marsh et al.	340/572
5,189,612	2/1993	Lemercier et al.	364/424.02	5,729,538	3/1998	Dent	370/347
5,196,846	3/1993	Brockelsby et al.	340/933	5,729,740	3/1998	Tsumura	395/615
5,278,759	1/1994	Berra et al.	364/424.01	5,749,984	5/1998	Frey et al.	340/444
5,289,369	2/1994	Hirshberg	340/825.34	5,758,300	5/1998	Abe	455/456
5,345,902	9/1994	Kalail, Sr. et al.	123/198 B	5,769,051	6/1998	Bayron et al.	123/335
5,379,042	1/1995	Henoch	340/825.54	5,803,043	9/1998	Bayron et al.	123/335
5,420,794	5/1995	James	701/117	5,809,142	9/1998	Hurta et al.	380/24
5,422,624	6/1995	Smith	340/438	5,894,266	4/1999	Wood, Jr. et al.	340/539
5,459,660	10/1995	Berra	364/424.03	5,995,898	11/1999	Tuttle	701/102
5,483,827	1/1996	Kulka et al.	73/146.5	6,006,148	12/1999	Strong	701/33

UNITED STATES PATENT AND TRADEMARK OFFICE

**CERTIFICATE OF CORRECTION**

PATENT NO. : 6,112,152

DATED : August 29, 2000

INVENTOR(S) : John R. Tuttle

It is certified that error appears in the above-identified patent and that said Letters Patent are hereby corrected as shown below:

Column 8, line 25, after "speed" insert --of the vehicle in response to receiving an adjustment signal from the interrogator via radio frequency--.

Signed and Sealed this

Eighth Day of May, 2001

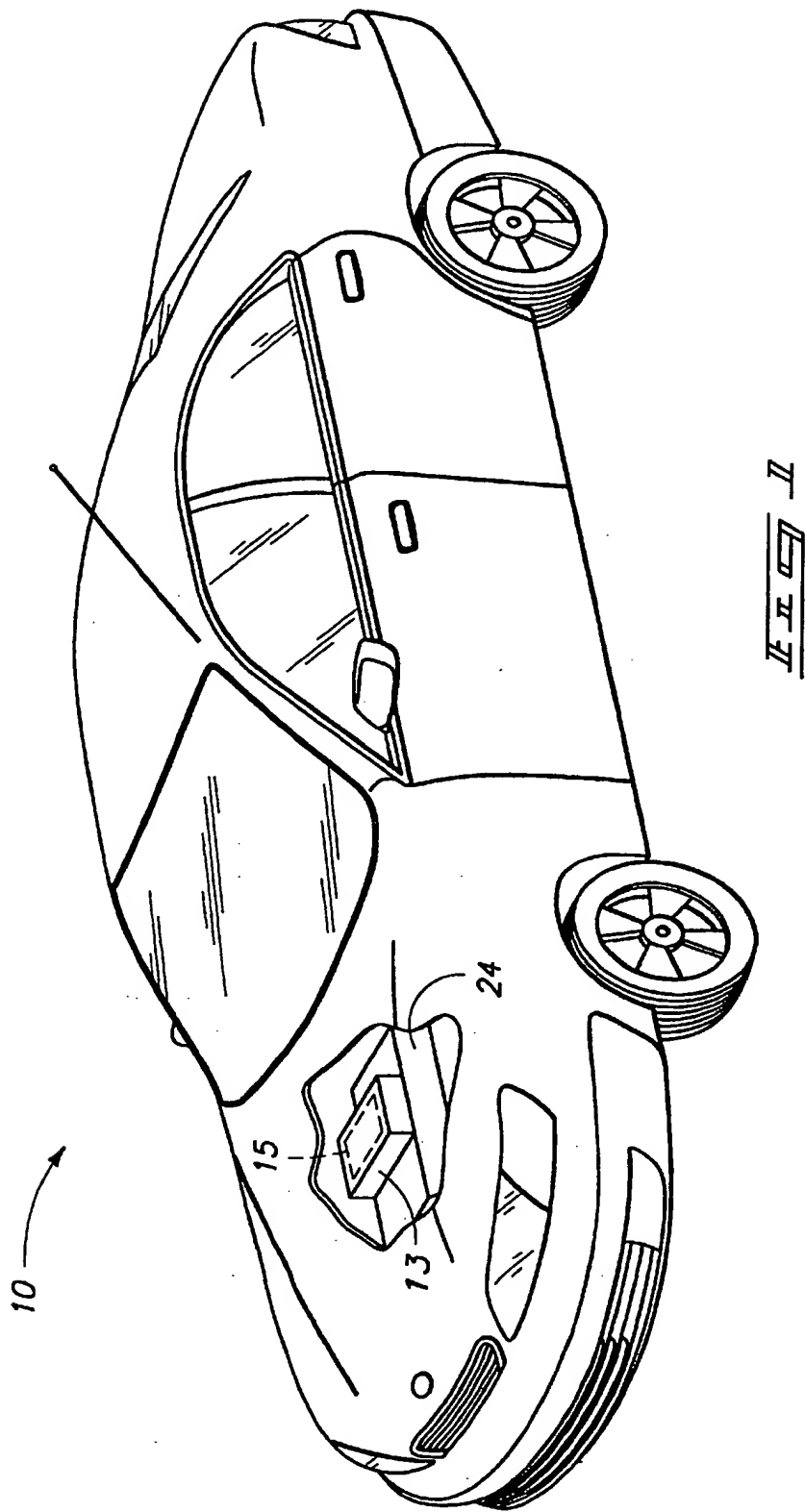
Attest:

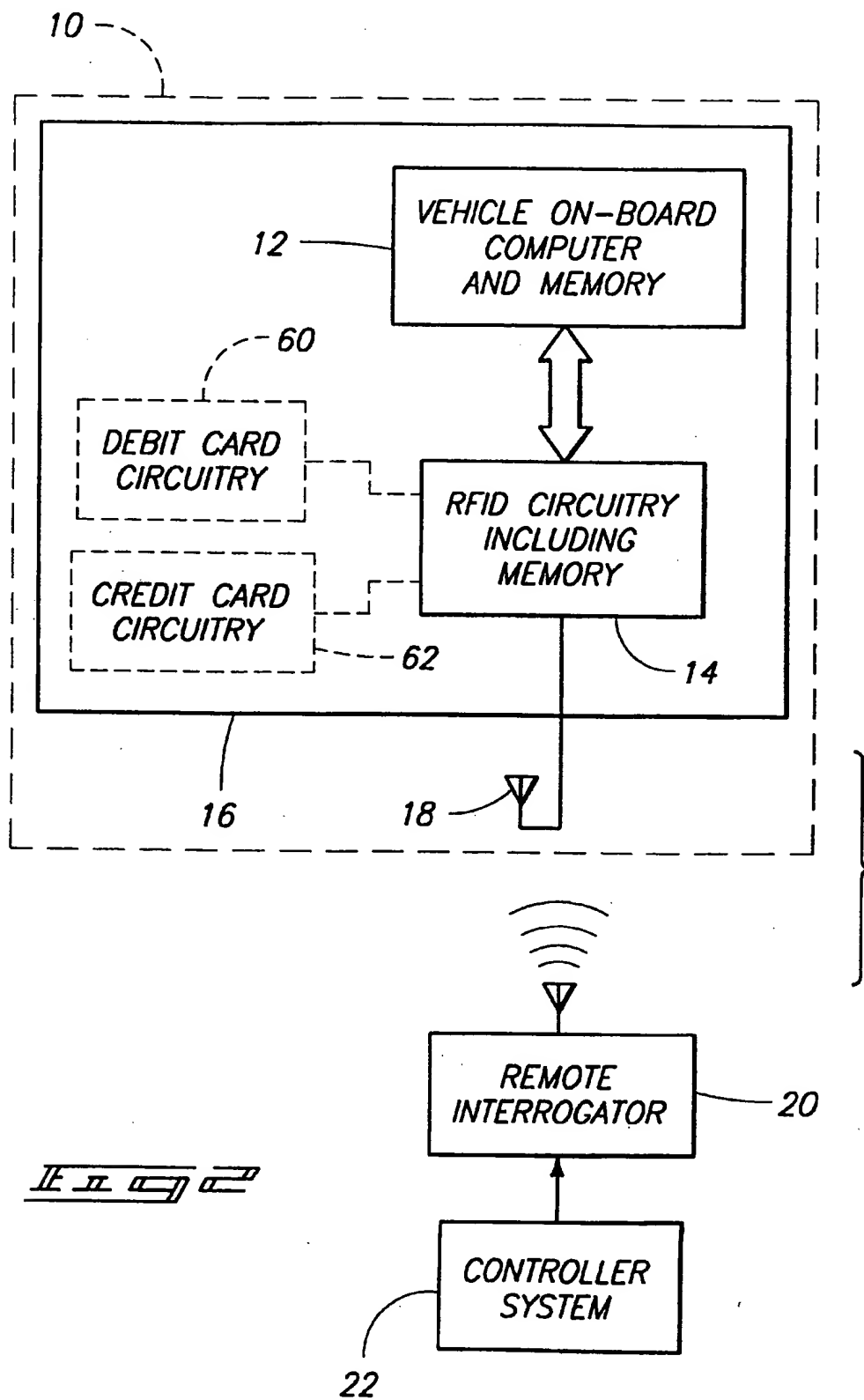
*Nicholas P. Godici*

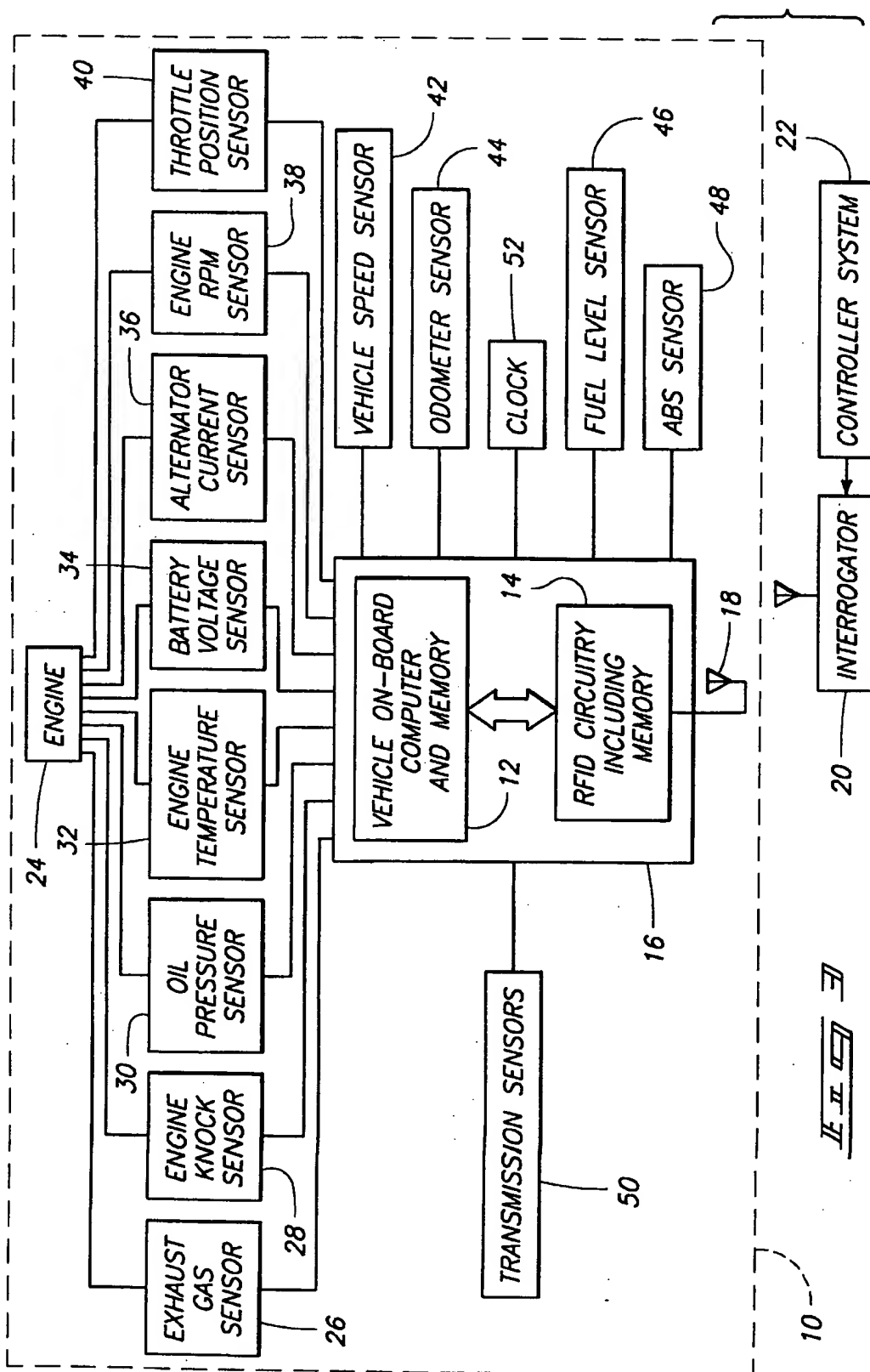
NICHOLAS P. GODICI

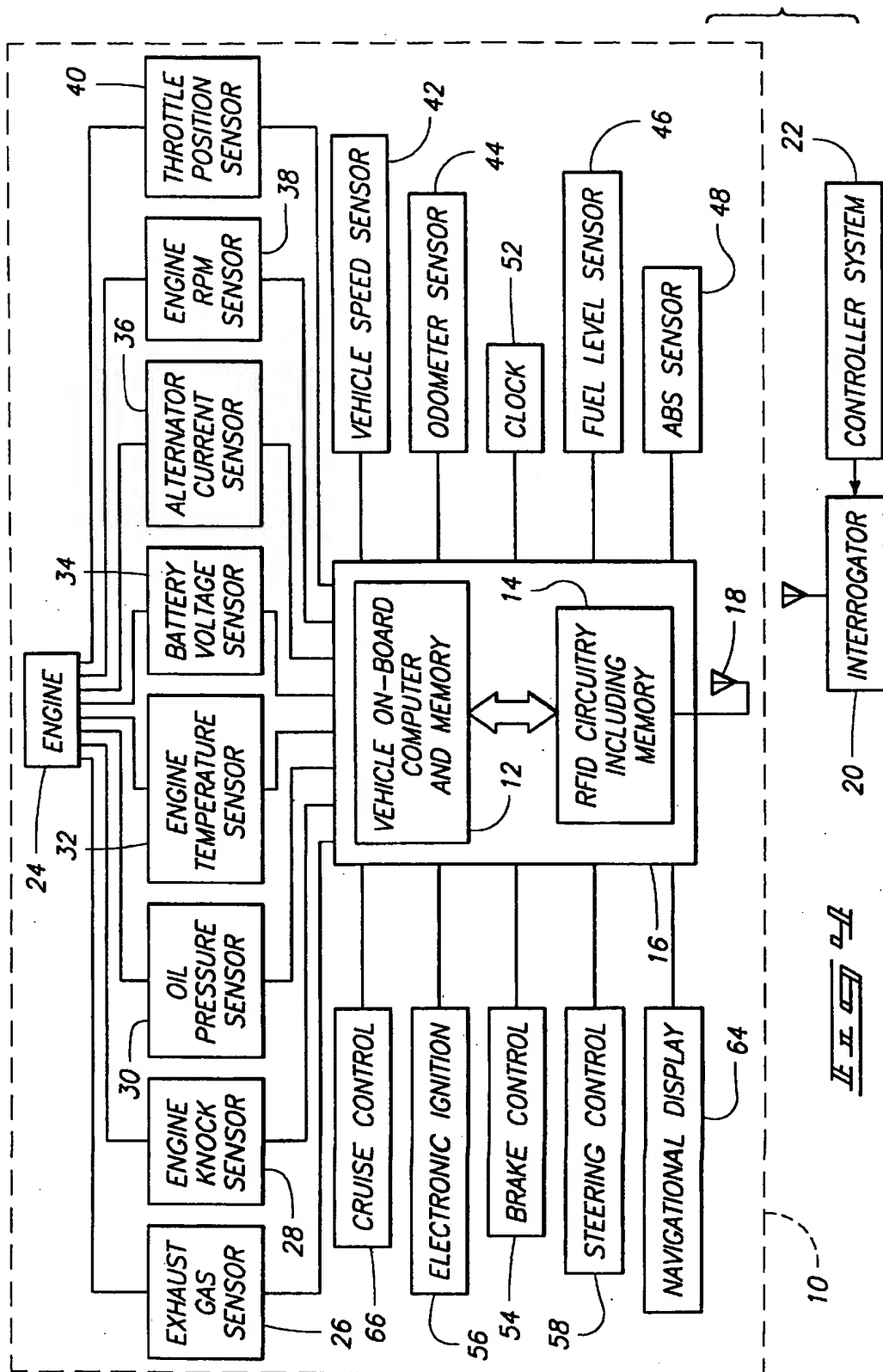
Attesting Officer

Acting Director of the United States Patent and Trademark Office









1

# RFID SYSTEM IN COMMUNICATION WITH VEHICLE ON-BOARD COMPUTER

## CROSS REFERENCE TO RELATED APPLICATION

This is a Continuation of U.S. patent application Ser. No. 08/759,737, filed Dec. 6, 1996, now U.S. Pat. No. 5,995,898, Issued Nov. 30, 1999, and titled "RFID System in Communication with Vehicle On-Board Computer".

## TECHNICAL FIELD

The invention relates to on-board vehicle computer systems and to radio frequency identification devices.

## BACKGROUND OF THE INVENTION

On-board vehicle computer systems are known in the art. Such systems monitor and control operations of mechanical vehicle systems, including vehicle engine systems, transmission systems, brake systems, suspension systems, and display systems. On-board computer systems receive information from various sensors, such as engine speed sensors, manifold pressure sensors, etc. The on-board computer systems can control systems such as by controlling mixture, fluid flow, etc., by controlling electronic systems, or by controlling solenoid-actuated valves that regulate flow of hydraulic fluid. One such computerized vehicle system is described in U.S. Pat. No. 4,875,391 to Leising et al. (incorporated by reference). A system for interfacing with a vehicle computer is disclosed in U.S. Pat. No. 5,459,660 to Berra (incorporated by reference); and a system for reprogramming vehicle computers is disclosed in U.S. Pat. No. 5,278,759 to Berra et al. (incorporated by reference). German Patent Document DE 35 40 599 A1 discloses an on-board vehicle computer having a display system that is arranged in an instrument cluster of a dashboard of a vehicle. An on-board computer for a motor vehicle is also disclosed in U.S. Pat. No. 5,150,690 to Ebner et al. (incorporated by reference).

Many vehicles employ several separate microprocessor based computer systems which cooperate with one another. On-board communications systems typically include data busses to enable data communication between such vehicle computer systems. Such data bus technology is disclosed in U.S. Pat. Nos. 4,706,082; 4,719,458; 4,739,323; 4,739,324; and 4,742,349 (all of which are incorporated by reference). Such communications systems may employ multiplexing so that simple wire harnesses can be employed for data transmission. In many vehicles, direct access may be provided to monitored data on a real time basis, so that display tools and engine analyzers may be used to perform a more complete diagnosis of engine problems than can be performed by on-board computers. For example, a data terminal connected to an input/output port of the vehicle computer or to an electronic control module may be provided under a dashboard, as described in U.S. Pat. No. 4,853,850 to Krass, Jr. et al. (incorporated by reference).

Because of heavy reliance on on-board computer systems, vehicles presently sold in the United States provide a standardized diagnostic interface according to a "OBDII/CARB" standards requirement. The OBDII/CARB requirement offers a choice between a J1850 specification and an ISO9141 (International Standards Organization) specification. The OBDII requirement, the J1850 standard, and the ISO9141 specification are incorporated herein by reference.

It is also known to use hand held display tools to display code values generated by vehicle computers. Such hand held display tools are described in U.S. Pat. No. 4,602,127 to Neely et al.

2

## SUMMARY OF THE INVENTION

A system comprising a vehicle on-board computer; and a wireless transponder device coupled to the vehicle on-board computer. The system performs a variety of functions because of its ability to transmit and receive data from other transponders which may be remote from the vehicle or located in the vehicle at a location spaced apart from the system. Remote transponders are spaced apart from the vehicle. The remote transponders can be positioned, for example, at a gas station, toll booth, service center, dealership, parking lot, or along a roadside.

## BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention are described below with reference to the following accompanying drawings.

FIG. 1 is a perspective view of a vehicle embodying the invention.

FIG. 2 is a block diagram illustrating a system in accordance with one embodiment of the invention.

FIG. 3 is a block diagram illustrating a system in accordance with a more particular embodiment of the invention.

FIG. 4 is a block diagram illustrating a system in accordance with an alternative embodiment of the invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

This disclosure of the invention is submitted in furtherance of the constitutional purposes of the U.S. Patent Laws "to promote the progress of science and useful arts" (Article 1, Section 8).

The figures show a vehicle 10 embodying the invention. The vehicle 10 includes an on-board computer (and memory) 12 in communication with wireless transponder circuitry 14 (FIG. 2). In the illustrated embodiment, the wireless transponder circuitry 14 comprises RFID circuitry including memory. In an alternative embodiment, the wireless transponder circuitry 14 comprises infrared transponder circuitry. One example of a vehicle on-board computer is disclosed in U.S. Pat. No. 4,875,391 to Berra (incorporated by reference). An example of RFID circuitry is disclosed in commonly assigned U.S. patent application Ser. No. 08/705,043, filed Aug. 29, 1996 (incorporated by reference).

In one embodiment, the RFID circuitry 14 and vehicle on-board computer 12 are provided in a common module or housing 13 that can be easily installed in or removed from a vehicle. Thus, the combination of the vehicle on-board computer memory 12, and the RFID circuitry including memory 14, can be used to replace existing vehicle on-board computers by swapping modules. The vehicle on-board computer 12, and the RFID circuitry 14 can also be installed as new equipment in new vehicles instead of as a retrofit item. In one embodiment, the RFID circuitry 14 is provided on a common (substantially planar) substrate 15 with the vehicle on-board computer (and memory) 12.

The RFID circuitry 14 includes, in the illustrated embodiment, an integrated circuit having a transmitter, a receiver, a microprocessor, and a memory.

In one embodiment, the RFID circuitry 14 is in serial communication with the vehicle on-board computer and memory 12. More particularly, the RFID circuitry 14 includes a serial data pin. Other forms of communication; e.g., using dual-ported RAM, can be employed. In one embodiment, the vehicle on-board computer and memory 12



is spaced apart in the vehicle from the RFID circuitry 14, and the RFID circuitry communicates with the vehicle on-board computer and memory 12 via a data communications bus such as that described in U.S. Pat. No. 4,853,850 to Krass, Jr. et al. (incorporated by reference), or U.S. Pat. No. 5,459,660 to Berra (incorporated by reference). The combination of the vehicle on-board computer and memory 12 and RFID circuitry 14 define a system 16.

The vehicle 10 further includes an antenna 18 connected to the RFID circuitry 14. The antenna 18 can either be supported by the system 16, or can be located at another location of the vehicle 10, and connected to the RFID circuitry 14 via a cable.

The RFID circuitry 14 communicates with a remote interrogator 20 controlled by a controller system 22.

The system 16 performs a variety of functions because of its ability to transmit and receive data from transponders 20. The transponders 20 may include remote transponders, or one or more transponders in the vehicle, but spaced apart from the system 16. The remote transponders 20 are typically interrogators which are spaced apart from the vehicle. The remote interrogators can be positioned, for example, at a gas station, toll booth, service center, dealership, parking lot, or along a roadside.

In another embodiment, the circuitry 14 defines an interrogator, and the transponders 20 define RFID circuits described in detail in U.S. patent application Ser. No. 08/705,043, and having unique identification codes. Thus, in this embodiment, the location of the interrogators and RFID devices is switched. In one embodiment, the RFID circuitry and an interrogator are both located on the same vehicle for data communications in the vehicle without using a standard data bus or wiring harness.

The system 16 provides for remote communication of the vehicle on-board computer for a variety of purposes.

For example, telemetry of vehicle performance data can be performed. More particularly, as shown in FIG. 3, the vehicle 10 includes a motor or engine 24, and the system 16 communicates with a plurality of sensors measuring various parameters of the motor 24, or of the vehicle 10 in general. Such sensors are typically read by the vehicle on-board computer 12; however, in alternative embodiments, sensors which are not read by the vehicle on-board computer 12 may be read directly by the RFID circuitry 14.

In one embodiment, the vehicle 10 is an electric vehicle, and the motor 24 is an electric motor. In this embodiment, the vehicle on-board computer 12 performs such functions as controlling power applied to the motor 24 based on angle of inclination of an accelerator actuator, controlling braking, controlling operation of a flywheel that stores mechanical energy on braking, and controlling other functions typically controlled in electric vehicles. For example, in one embodiment, the on-board computer 12 controllably reduces power delivery to the motor during braking, so that braking in response to actuation of a brake pedal is gradual and feels like braking in a more conventional vehicle of the type including an internal combustion engine.

In another embodiment, the motor 24 is an internal combustion engine.

In the embodiment shown in FIG. 3, the sensors include any or all of the following sensors: an exhaust gas sensor 18 (or O<sub>2</sub> sensor), an engine knock sensor 28, an oil pressure sensor 30, an engine temperature sensor 32, a battery voltage sensor 34, an alternator current sensor (or charging amps sensor) 36, an engine RPM sensor (or tachometer) 38, an accelerator pedal or throttle position sensor 40, a vehicle

speed sensor 42, an odometer sensor 44, a fuel level sensor 46, an ABS braking system sensor 48, transmission sensor 60, a clock 52, and any other sensors typically employed with vehicle on-board computers, or that can be employed with vehicle on-board computers. In one embodiment, the clock 52 is incorporated in the vehicle on-board computer 12 or in the RFID circuitry 14. In one embodiment, the vehicle 10 includes, in communication with the system 16, systems and sensors such as those described in the following patents (all of which are incorporated herein by reference): U.S. Pat. No. 4,168,679 to Ikeura et al.; U.S. Pat. No. 4,237,830 to Stivender; U.S. Pat. No. 4,335,695 to Phipps; U.S. Pat. No. 4,524,745 to Tominari et al.; and U.S. Pat. No. 4,552,116 to Kuroiwa et al.

Thus, the system 16 can be used to remotely convey vehicle performance data measured by the sensors. It is now possible, therefore, for a garage or service station to diagnose a problem with the vehicle 10 without needing to physically connect diagnostic equipment to the vehicle 10. It is possible for a garage to begin to diagnose a problem with the vehicle as the vehicle is driven into the service station. In one embodiment, the system 16 includes information identifying the vehicle or the owner of the vehicle. In this embodiment, the garage or service station will know the name of the owner of the vehicle as the owner drives in to the service station, before the owner gets out of the vehicle.

In one embodiment using the system 16, vehicle history is logged in memory (either in the vehicle on-board computer 12, or in the RFID circuitry 14). For example, the vehicle on-board computer can be programmed to periodically store readings from any or all of the various sensors 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 52, 46, 48, and 50. This information can then be read remotely after the information has been logged.

In one embodiment, the system 16 is used in a rental vehicle facility. In this embodiment a unique code identifying a vehicle is stored in memory in the system 16, and a remote transponder is located at a controlled access point of a rental car return facility. When the vehicle is returned, the remote transponder communicates with the RFID circuitry 14 so as to remotely receive the vehicle identifying data when the vehicle passes the controlled access point. In one embodiment, the remote transponder receives mileage information from the returned vehicle. In another embodiment, the remote transponder receives fuel level information from the returned vehicle. Using such information, a bill can be calculated immediately, reducing human labor needed at car rental facilities. The system 16 can also be used to log, via remote communications with a remote transponder, when a rental vehicle leaves the rental facility (using the unique identification code), so that the start of the rental period can be determined automatically.

Further, information can be transmitted to memory (either in the vehicle on-board computer 12, or in the RFID circuitry 14) remotely. Such information can include vehicle history information including maintenance records, ownership data, purchase price for the vehicle, purchase date of the vehicle, option packages installed at the factory, options added to the vehicle after purchase, warranty records, or other information.

In one embodiment, the system 16 is used as a remote access credit or debit card. This may be particularly convenient for purchasing items associated with vehicles, such as fuel, oil, maintenance, etc., for payment of toll or parking garage payment, or for payment of cellular phone time. In

this embodiment, some form of access control is provided to the portion of the memory in the system 16 which contains credits for the debit card. These credits can be incremented remotely, by a remote transponder 20, which possesses a password to gain access to the portion of memory containing the credits for the debit card. Such a password would normally be held, for example, by a bank, or credit union, or other service provider which accepts the debit card. In this embodiment, the system 16 is programmed to operate as a conventional debit card, except that payment can be made remotely using the RFID circuitry 14. After payment is made, by reducing the credit balance in the memory, the RFID circuitry 14 indicates to the remote transponder 20 seeking payment that payment has been made.

The system 16 can also be used as a credit card (such as a oil company/gasoline credit card, or a bank-issued credit card). In this embodiment, credit card account information, including a credit card number is stored in the memory of the system 16 and is transmitted by the RFID circuitry 14 to a transponder 20 to make a payment. Other information that may be stored and transmitted include expiration date, cardholder name, zip code, cardholder billing address, bank name, bank phone number, etc. If the system 16 is being used as a credit card, payment history or purchase history may be stored in the memory of the system 16.

If the system 16 is used as a debit card, the appropriate programming and access control defines debit card circuitry 60. If the system 16 is used as a credit card, the account number information and programming defines credit card circuitry 62.

The system 16 is also used, in one embodiment, as an intelligent roadside communications link for intelligent highway applications, or intelligent transportation systems. For example, if the vehicle 10 approaches a stop sign having a transponder 20, the RFID circuitry 14 will recognize that the vehicle is approaching a stop sign, and will sound an alarm in the vehicle 10, or may effect application of the brakes of the vehicle or reduction in vehicle speed. In this embodiment, the vehicle 10 includes a brake control system 54 (FIG. 4) that selectively applies the brakes in response to an appropriate command from a transponder 20. In one embodiment, where the vehicle 10 includes an internal combustion engine, the vehicle 10 includes an electronic ignition system 56 that selectively reduces vehicle speed in response to an appropriate command from a transponder 20. In another embodiment, where the vehicle 10 is an electric vehicle, the vehicle includes a braking system (as described above) that selectively reduces vehicle speed in response to an appropriate command from a transponder 20 (such as by reducing power applied to the electric motor, or by transferring mechanical energy to a flywheel).

In one embodiment, the system 16 uses signal strength to determine vehicle distance relative to the transponder 20. This information is used, in one embodiment, to determine whether to merely reduce engine speed, or to apply brakes. In one embodiment, distance is used by the system to determine what level of braking should be employed, and this information is used to appropriately control the brake control system 54.

In one embodiment, the RFID circuitry 14 transmits the speed of the vehicle for monitoring by police. In an alternative embodiment, a transponder 20 transmits a signal warning of dangerous road conditions, such as fog, flooding, or an accident ahead, which signal is received by the RFID circuitry 14, and causes the vehicle on-board computer 12 to reduce the speed of the engine or limit the speed of the

vehicle or limit the RPM of the engine or downshift the transmission, overriding user actuable controls (e.g. accelerator), etc. In this embodiment, the speed of the vehicle 10 is controlled by the electronic ignition 56 (for vehicles with internal combustion engines), by a motor control system (for electric vehicles), or the vehicle 10 includes a cruise control system 66 controlling the speed of the vehicle 10.

In another embodiment, speed limit signs include transponders 20 transmitting a signal indicative of maximum speed for the road or highway, which signals are received by the RFID circuitry 14, and communicated to the vehicle on-board computer and memory 12, which limits vehicle speed to the received speed limit. Alternatively, the vehicle includes an actuator allowing the driver to set a vehicle speed relative to the speed received by the speed limit transponder.

Two tiered speed transponders can also be employed, including transponders transmitting a recommended speed (e.g., around curves, etc.), and other transponders transmitting speed limit information. In this embodiment, the vehicle includes actuators for selecting controlling vehicle speed relative to one or the other type of speed transponders 20.

In another embodiment, transponders 20 are positioned along a roadway, and the system 16 uses these signals to determine its position and to maintain the vehicle within certain bounds; e.g., if the driver falls asleep at the wheel, or desires to relinquish steering control. In this embodiment, the vehicle 10 includes a steering control system 58 which controls steering of the vehicle. In one embodiment, the system is a safety system which overrides the user actuable control (e.g. steering wheel) when the system 16 determines that the vehicle is about to go off the road. Such a steering control system can be turned on or off by the user. For example, the user (driver) selectively turns on the steering control system 58 upon entering a highway, and turns off the steering control system 58 if he or she desires to leave the highway or to pull off the road. The steering control system 58 can also be used for completely automated steering of a passenger vehicle, receiving signals from the transponders 20 along the road to guide the vehicle 10. Such a system may be similar to the system described in U.S. Pat. No. 5,189,612 (incorporated herein by reference) except that radio frequency transponders are employed instead of buried magnetic markers. In one embodiment, the vehicle may be a remotely controlled tractor or robot vehicle as opposed to a passenger vehicle.

Using a transponder 20, information from external sources can be transferred to the system 16 for various applications. In one embodiment, information is transferred to the system 16 for such applications as remote service adjustments of the engine 24, e.g., by adjusting the electronic ignition 56. In one embodiment, a transponder 20 is used for remote loading of debit card data or credits. In one embodiment, a transponder 20 is used for remote control of the brakes or steering (as described above). In one embodiment, a transponder 20 is used to transfer travel information to the vehicle (e.g., indicating what services are available at the next exit, indicating distances to various points, etc.).

In one embodiment, navigational maps or data from maps are transmitted to the system 16 by a remote transponder 20 at various locations (e.g., upon entering a state or city). In such embodiments, the vehicle 10 includes a navigational display 64 displaying maps selected by the user or driver including maps of the particular area in which the user or

7

driver is presently driving, and plotting items such as gasoline stations, motels, restaurants, or other providers of goods or services. The system 16, if requested, determines which map to display, determines where the vehicle 10 is located, and plots the location of the vehicle on a map or choose an appropriate map for the location of the vehicle.

More particularly, in one embodiment, transponders 20 each have their own identification codes, and the RFID circuitry 14 determines where the vehicle 10 is located (e.g., using triangulation) based on when the RFID circuitry 14 communicated with one or more particular transponders, the location of those transponders, and the speed of the vehicle 10 as read by the speed sensor (and, in one embodiment, based on signal strength or rate of change of signal strength).

Similarly, state agencies or friends or relatives can determine the position of a particular vehicle 10.

More particularly, different vehicles 10 include different unique identification codes stored in the system 16, and these identification code are transmitted to transponders 20 as the vehicles pass within communications range of these transponders 20. A system external to the vehicle can determine (e.g., using triangulation) the location of the vehicle based on when a particular vehicle's system 16 communicated with particular transponders 20, the location of those transponders 20, and the speed of the vehicle as read by the speed sensor 42 (and, in one embodiment, based on signal strength or rate of change of signal strength).

This unique identification code can also be used for other purposes, such as for informing garages or maintenance facilities of the name of the vehicle owner as the vehicle pulls into the maintenance facility. The unique identification code can also be used in toll systems, parking lots, or other pay systems in which the system 16 does not act as a debit card. More particularly, a transponder at a toll booth, parking lot, etc., reads the unique identification code and debits an account associated with that particular identification code.

Various other applications for the system 16 will readily be apparent to those of ordinary skill in the art.

In compliance with the statute, the invention has been described in language more or less specific as to structural and methodical features. It is to be understood, however, that the invention is not limited to the specific features shown and described, since the means herein disclosed comprise preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims appropriately interpreted in accordance with the doctrine of equivalents.

What is claimed is:

1. An electric vehicle comprising:

a battery;

an electric motor coupled to the battery to receive power from the battery;

a sensor measuring a parameter of the electric motor;

a vehicle on-board computer; and

a radio frequency transponder in communication with the vehicle on-board computer and transmitting information measured by the sensor by radio frequency in response to a radio frequency interrogation by an interrogator.

2. An electric vehicle comprising:

an electric motor;

a control system controlling the electric motor;

a sensor providing a signal indicative of speed of the vehicle;

8

a vehicle on-board computer in communication with the control system and selectively causing the control system to adjust at least one operating parameter of the electric motor; and

a radio frequency transponder in communication with the vehicle on-board computer, and causing the control system to adjust the operating parameter of the electric motor to reduce speed of the vehicle in response to receiving an adjustment signal from the interrogator via radio frequency.

3. A vehicle comprising:

an internal combustion engine;

a control system controlling the internal combustion engine;

a sensor providing a signal indicative of speed of the vehicle;

a vehicle on-board computer in communication with the control system and selectively causing the control system to adjust at least one operating parameter of the internal combustion engine; and

a radio frequency transponder in communication with the vehicle on-board computer, and causing the control system to adjust the operating parameter of the internal combustion engine to reduce speed.

4. A vehicle comprising:

an internal combustion engine;

a control system controlling at least one operating parameter of the internal combustion engine;

a plurality of sensors measuring a plurality of parameters of the internal combustion engine;

a vehicle on-board computer in communication with the control system and selectively causing the control system to adjust the at least one operating parameter of the internal combustion engine; and

a radio frequency transponder in communication with the vehicle on-board computer and transmitting information measured by the sensors by radio frequency in response to a radio frequency interrogation by an interrogator, and causing the on-board computer to adjust the at least one operating parameter of the internal combustion engine in response to receiving an adjustment signal from the interrogator via radio frequency.

5. A vehicle in accordance with claim 4 and further comprising an electronic ignition system in communication with the internal combustion engine and controlling timing of the internal combustion engine, and wherein the on-board computer adjusts timing of the internal combustion engine in response to receiving an adjustment signal from the interrogator via radio frequency.

6. A vehicle in accordance with claim 4 wherein the sensors comprise an exhaust sensor.

7. A vehicle in accordance with claim 4 wherein the sensors comprise an engine knock sensor.

8. A vehicle in accordance with claim 4 wherein the sensors comprise an engine RPM sensor.

9. A system for telemetry of vehicle performance data in a vehicle including an internal combustion engine, the system comprising:

a vehicle on-board computer;

a radio frequency transponder in communication with the vehicle on-board computer, the radio frequency transponder including an integrated circuit having a transmitter, a receiver, and a microprocessor coupled to the transmitter and receiver;

an engine temperature sensor configured to measure the temperature of the engine; and

a battery voltage sensor, wherein the radio frequency transponder is configured to transmit information measured by a selected one of the sensors by radio frequency transmission in response to a radio frequency interrogation by an interrogator and depending on what information is requested by the interrogator.

10. A system for telemetry of vehicle performance data, the system comprising:

a vehicle on-board computer system;

a radio frequency identification device in communication with the on-board computer system, the radio frequency identification device including an integrated circuit having a transmitter, a receiver, and a micro-processor;

an oil pressure sensor, the oil pressure sensor being in communication with the on-board computer system and configured to communicate oil pressure to the on-board computer system,

the radio frequency identification device transmitting the data communicated to the on-board computer system in response to a radio frequency interrogation being received by the radio frequency identification device from an interrogator; and

a battery voltage sensor, wherein the radio frequency transponder transmits information measured by a selected one of the sensors by radio frequency in response to a radio frequency interrogation by an interrogator and depending on what information is requested by the interrogator.

11. A method of logging vehicle history, the method comprising:

supporting a memory in a vehicle, the vehicle having a transmission;

coupling a wireless communication device to a vehicle on-board computer of the vehicle, the wireless communication device including an integrated circuit having a transmitter, and a receiver coupled to the memory; periodically storing information representative of transmission performance in the memory; and

communicating with the wireless communication device to read the data representative of transmission performance from the memory from a location spaced apart from the vehicle.

12. A method in accordance with claim 11 and further comprising storing data representative of transmission performance in the memory and selectively reading the data representative of transmission performance from the memory via wireless communications.

13. A method in accordance with claim 11 and further comprising storing a vehicle maintenance record in the memory and selectively reading the vehicle maintenance record from the memory via wireless communications.

14. A method in accordance with claim 11 and further comprising storing information identifying the owner of the vehicle in the memory and selectively reading the information identifying the owner from the memory via wireless communications.

15. A method in accordance with claim 11 and further comprising storing information indicative of the purchase price of the vehicle in the memory and selectively reading the information indicative of purchase price from the memory via wireless communications.

16. A method in accordance with claim 11 and further comprising storing information indicative of the purchase

date of the vehicle in the memory and selectively reading the information indicative of purchase price from the memory via wireless communications.

17. A method in accordance with claim 11 and further comprising storing information indicative of vehicle installed options in the memory and selectively reading the information indicative of vehicle installed options from the memory via wireless communications.

18. A method in accordance with claim 11 and further comprising storing information indicative of repairs made to the vehicle and selectively reading the information indicative of repairs from the memory via wireless communications.

19. A method of logging vehicle history, the method comprising:

providing a memory in a vehicle, the vehicle having an engine and a vehicle on-board computer coupled to the engine;

coupling a wireless communication device to the vehicle on-board computer, the wireless communication device including an integrated circuit having a transmitter, a receiver;

periodically storing information from the vehicle on-board computer in the memory; and

communicating with the wireless communication device and reading from the memory at a location spaced apart from the vehicle.

20. A method in accordance with claim 19 and further comprising storing data representative of engine performance in the memory and selectively reading the data representative of engine performance from the memory via wireless communications.

21. A method in accordance with claim 19 and further comprising storing a vehicle maintenance record in the memory and selectively reading the vehicle maintenance record from the memory via wireless communications.

22. A method in accordance with claim 19 and further comprising storing information identifying the owner of the vehicle in the memory and selectively reading the information identifying the owner from the memory via wireless communications.

23. A method in accordance with claim 19 and further comprising storing information indicative of the purchase price of the vehicle in the memory and selectively reading the information indicative of purchase price from the memory via wireless communications.

24. A method in accordance with claim 19 and further comprising storing information indicative of the purchase date of the vehicle in the memory and selectively reading the information indicative of purchase price from the memory via wireless communications.

25. A method in accordance with claim 19 and further comprising storing information indicative of vehicle installed options in the memory and selectively reading the information indicative of vehicle installed options from the memory via wireless communications.

26. A method in accordance with claim 19 and further comprising storing information indicative of repairs made to the vehicle and selectively reading the information indicative of repairs from the memory via wireless communications.

27. A method of logging data from vehicles, the method comprising:

providing a system including a radio frequency transponder device, and a vehicle on-board computer in a vehicle, the radio frequency transponder device includ-

ing an integrated circuit having a memory configured to store data identifying the vehicle and having a microprocessor coupled to the memory;  
 providing a mileage sensor in the vehicle, in communication with the radio frequency transponder device, the mileage sensor being configured to generate mileage information;  
 locating a remote transponder at a controlled access point of a vehicle facility; and  
 causing the remote transponder to communicate with the radio frequency transponder device so as to receive via wireless communications the identifying data and mileage information when the vehicle passes the controlled access point and thereby determine that the vehicle has passed the controlled access point.

28. A method in accordance with claim 27 and further comprising providing an additional sensor in communication with the radio frequency transponder device, and causing the remote transponder to communicate with the radio frequency transponder device so as to receive via wireless communications data sensed by the additional sensor when the vehicle passes the controlled access point.

29. A method in accordance with claim 28 wherein the additional sensor is a fuel level sensor.

30. A method in accordance with claim 28 wherein the additional sensor is an oil pressure sensor.

31. A method in accordance with claim 28 wherein the additional sensor is an engine knock sensor.

32. A method in accordance with claim 28 wherein the additional sensor is an engine temperature sensor.

33. A method in accordance with claim 28 wherein the additional sensor is an exhaust gas sensor.

34. A method in accordance with claim 28 wherein the additional sensor is a battery voltage sensor.

35. A method in accordance with claim 28 wherein the additional sensor is an alternator current sensor.

36. A vehicle system for communicating with radio frequency interrogators provided along a road or highway, the system receiving a signal indicative of vehicle speed from a speed sensor, the system comprising:

- a vehicle on-board computer in communication with the speed sensor; and
- a radio frequency identification device in communication with the vehicle on-board computer, the radio frequency identification device providing an identification code identifying the vehicle;

the radio frequency identification device being operable to transmit the identification code to interrogators that the vehicle passes and receives information from the interrogator representative of the location of the interrogator;

wherein the on-board computer predicts the present location of the vehicle based on when the radio frequency identification device communicated with interrogators, the locations of those interrogators, and the speed of the vehicle read by the speed sensor.

37. A method of determining the location of a vehicle, the method comprising:

- providing a plurality of radio frequency interrogators at various locations;
- providing a radio frequency identification device in the vehicle, the radio frequency identification device including an integrated circuit having a memory, a transmitter, a receiver, and a microprocessor, and providing an identification code identifying the vehicle;
- causing individual interrogators to determine the identification code when the vehicle passes sufficiently close

- to the individual interrogators that the radio frequency identification device is within communication range;
- storing the time the vehicle passed a given interrogator; and
- predicting the present location of the vehicle based on when the radio frequency identification device communicated with individual interrogators and the locations of those individual interrogators.

38. A method of determining the location of a vehicle, the method comprising:

- providing a plurality of radio frequency interrogators at various locations;
- providing a vehicle speed sensor in the vehicle;
- providing a vehicle on-board computer in communication with the speed sensor;
- connecting a radio frequency identification device to the vehicle on-board computer, the radio frequency identification device providing an identification code identifying the vehicle;
- causing individual interrogators to determine the identification code when the vehicle passes sufficiently close to the interrogator that the radio frequency identification device is within communication range;
- storing the time the vehicle passed a given interrogator; and
- predicting the present location of the vehicle based on when the radio frequency identification device communicated with individual interrogators, the locations of those individual interrogators, and the speed of the vehicle read by the speed sensor.

39. An automatic parking fee payment system for a vehicle, for paying a parking fee and gaining access to a parking lot while the vehicle moves, comprising:

- a vehicle on-board computer system;
- a radio frequency transponder device in communication with the on-board computer system, the radio frequency transponder device including an integrated circuit having a transmitter, a receiver, and a microprocessor;
- a memory storing a credit balance, the system being configured to reduce the credit balance being reduced when the radio frequency transponder device receives a radio frequency communication indicating that parking payment is due, the radio frequency transponder device communicating to the parking lot that payment for parking was made; and
- circuitry which restricts access to the memory such that available credit can only be increased using a password.

40. A method of paying for vehicle maintenance, the method comprising:

- supporting a radio frequency transponder device on the vehicle, the radio frequency identification device including a single integrated circuit having a transmitter, receiver, memory, and microprocessor, the radio frequency transponder device including a memory storing a credit balance; and

13

causing the radio frequency transponder to selectively reduce the credit balance in response to a radio frequency command from an interrogator indicating that payment is due for maintenance supplied to the vehicle.

41. A method of paying for vehicle maintenance, the method comprising:

supporting a radio frequency transponder device from the vehicle, the radio frequency identification device including a single integrated circuit having a transmitter, receiver, memory, and microprocessor, the

14

radio frequency transponder device including debit card information and a memory storing a credit balance; and

causing the radio frequency transponder to selectively reduce the credit balance in response to a radio frequency command from an interrogator indicating that payment is due for maintenance supplied to the vehicle.

\* \* \* \* \*



US006175308B1

(12) **United States Patent**  
Tallman et al.

(10) **Patent No.:** US 6,175,308 B1  
(45) **Date of Patent:** Jan. 16, 2001

(54) **PERSONAL DURESS SECURITY SYSTEM**

(75) **Inventors:** Erven Tallman, Rancho Mirage, CA (US); Dan Minardi, Arvada; Jeff Hill, Aurora, both of CO (US)

(73) **Assignee:** Actall Corporation, Tustin, CA (US)

(\*) **Notice:** Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

(21) **Appl. No.:** 09/005,564

(22) **Filed:** Jan. 12, 1998

**Related U.S. Application Data**

(63) Continuation of application No. 08/167,216, filed on Dec. 16, 1993, now Pat. No. 5,708,417.

(51) **Int. Cl.<sup>7</sup>** ..... G08B 1/08

(52) **U.S. Cl.** ..... 340/539; 340/825.49; 340/825.34; 340/825.36; 340/825.72; 340/573.1; 340/573.4; 359/145; 359/152; 359/172

(58) **Field of Search** ..... 340/525, 573.1, 340/573.4, 825.49, 825.36, 825.34, 825.72, 539; 359/145

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

4,727,600	2/1988	Avakian .	
4,918,432 *	4/1990	Pauley et al. ....	340/573.4
4,978,946	12/1990	Nordolm et al. .	
4,990,892	2/1991	Guest et al. .	
4,998,095	3/1991	Shields .	
5,027,314	6/1991	Linwood et al. .	
5,045,839	9/1991	Ellis et al. .	
5,103,108	4/1992	Crimmins .	
5,153,584	10/1992	Engira .	
5,204,687	4/1993	Elliot et al. .	
5,218,344 *	6/1993	Ricketts .	340/573.1
5,223,816	6/1993	Levinson et al. .	
5,239,296	8/1993	Jenkins .	

5,268,734 12/1993 Parker et al. .  
5,301,353 4/1994 Borras et al. .  
5,317,309 5/1994 Vercellotti et al. .

(List continued on next page.)

**OTHER PUBLICATIONS**

1994 teleProtect 900, System Description.  
teleProtect 900, You'll Never Work Along With A Personal Alarm System.

Apr. 27, 1994, Harris Communications, promoting teleProtect 900.

\* cited by examiner

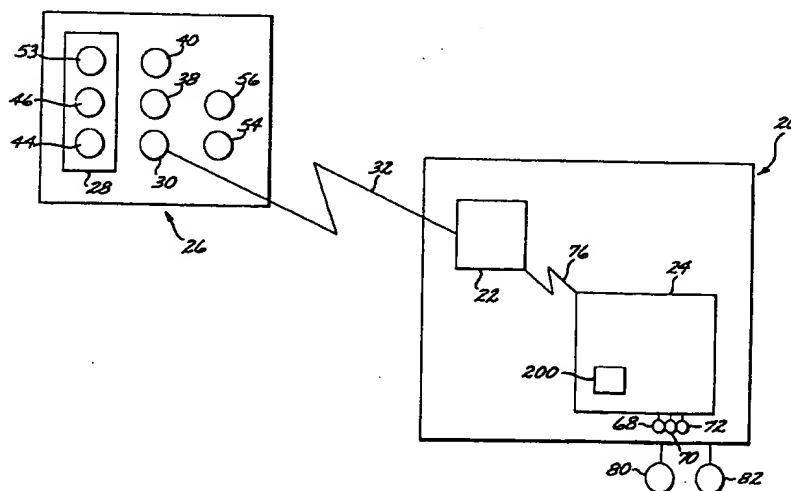
*Primary Examiner*—Daryl Pope

(74) *Attorney, Agent, or Firm*—Fulwider Patton Lee & Utecht, LLP

(57) **ABSTRACT**

A security system including tracking units or readers carried or mounted on mobile units to operatively communicate status signals indicating identity, location, direction of travel, and a number of alarm conditions to a local monitoring station. The tracking units or readers are equipped with an infrared receiver to receive infrared location signals transmitted by fixed infrared transmitters located throughout the area to be monitored. Each infrared transmitter transmits a unique location signal. The tracking unit is operative to transmit a radio frequency watchdog signal that includes the last two location signals received, indicating the time lapsed since receipt of those location signals, a unique identification signal indicative of the and any applicable alarm signals triggered by predetermined conditions to which the tracking unit is also operative to detect. The monitoring station includes a computer which is operative to receive the watchdog signal by way of radio frequency receivers located throughout the area being monitored and translate the watchdog signal into useful displays including printed text on a printer, computer monitor graphic and text displays, and audible alarms.

53 Claims, 11 Drawing Sheets



## U.S. PATENT DOCUMENTS

5,319,698	6/1994	Glidewell et al. .	5,552,772	9/1996	Janky et al. .
5,365,217	11/1994	Toner .	5,627,524	5/1997	Fredrickson et al. .
5,396,224	3/1995	Dukes et al. .	5,640,157	6/1997	Langeraar .
5,416,468	5/1995	Baumann .	5,650,769	7/1997	Campana .
5,426,425	6/1995	Conrad et al. .	5,652,570	• 7/1997	Lepkofker ..... 340/573
5,479,408	12/1995	Will .	5,689,229	11/1997	Chaco et al. .
5,485,163	1/1996	Singer et al. .	5,771,002	• 6/1998	Creek et al. .... 340/539
			5,917,425	• 6/1999	Crimmins ..... 340/825.49



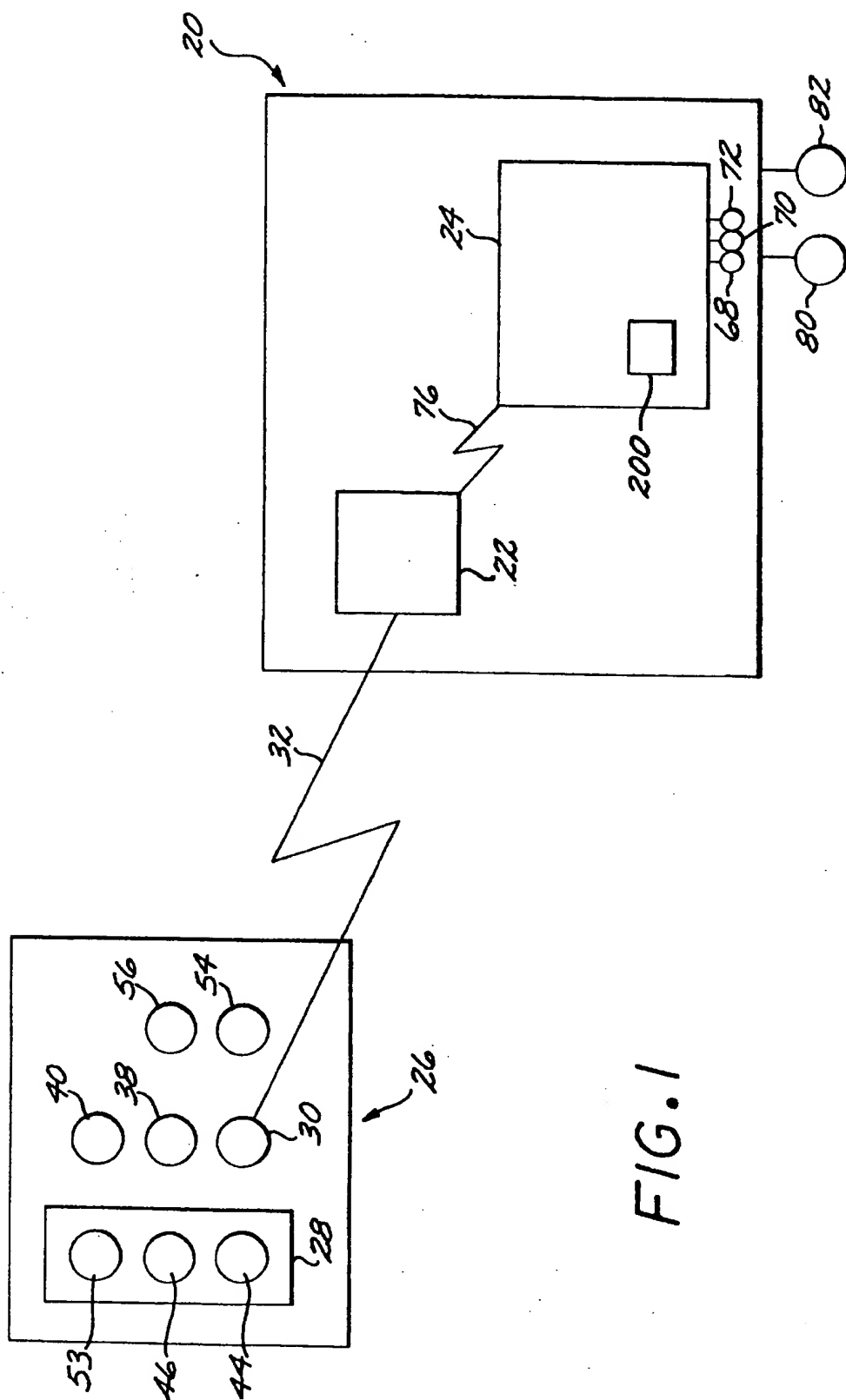


FIG. 1

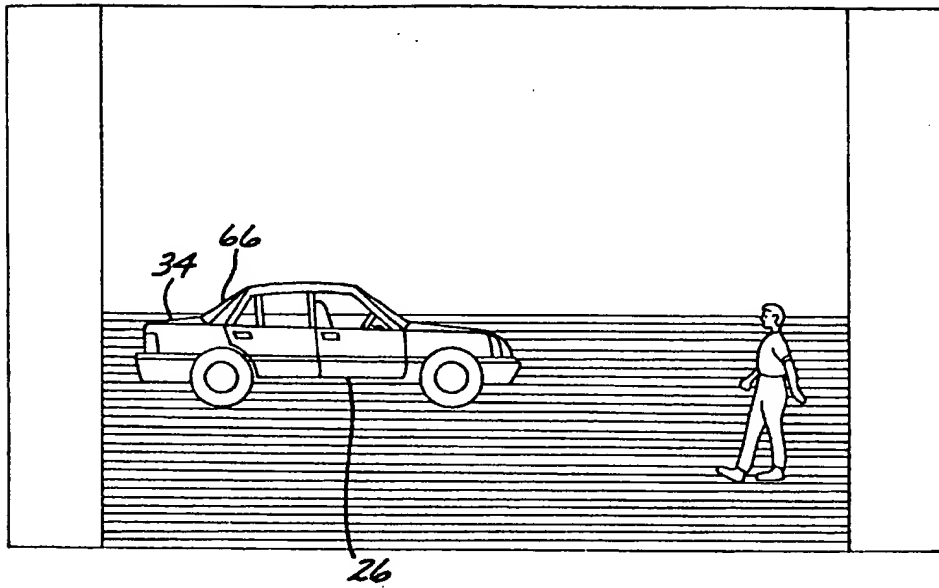


FIG. 2

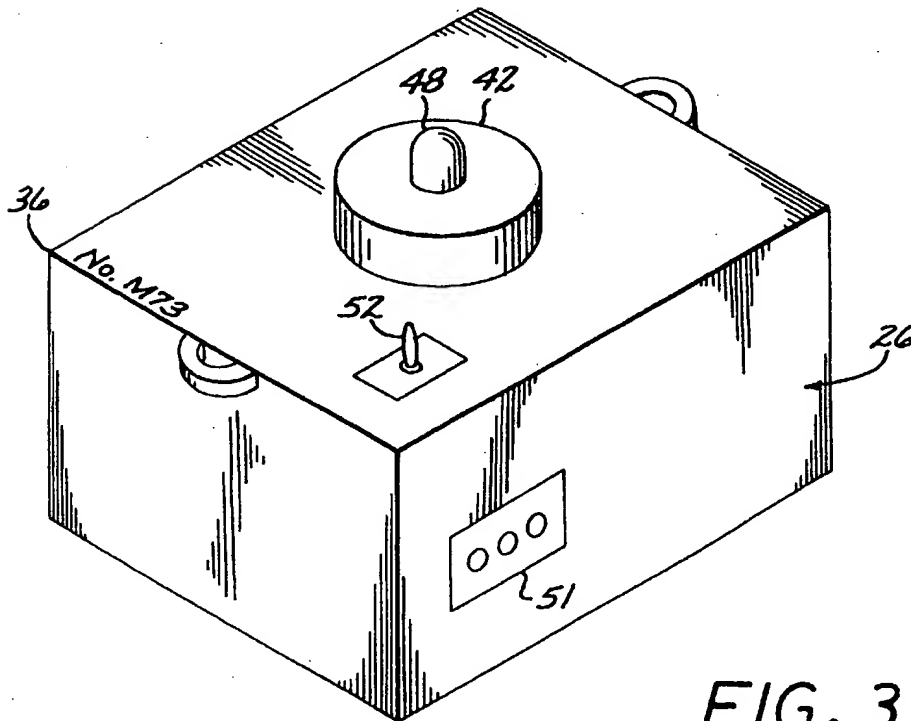


FIG. 3

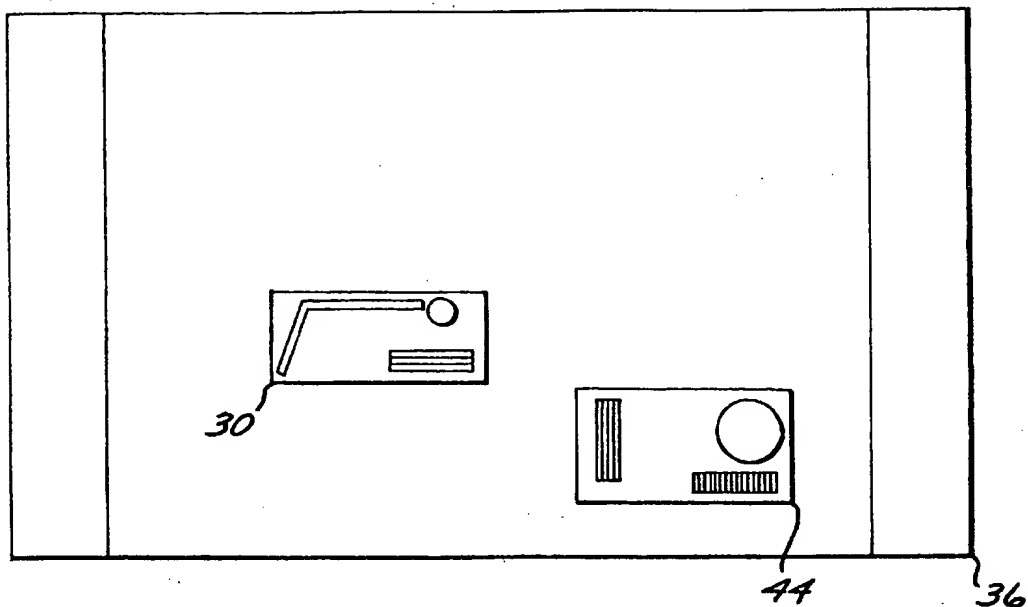


FIG. 4

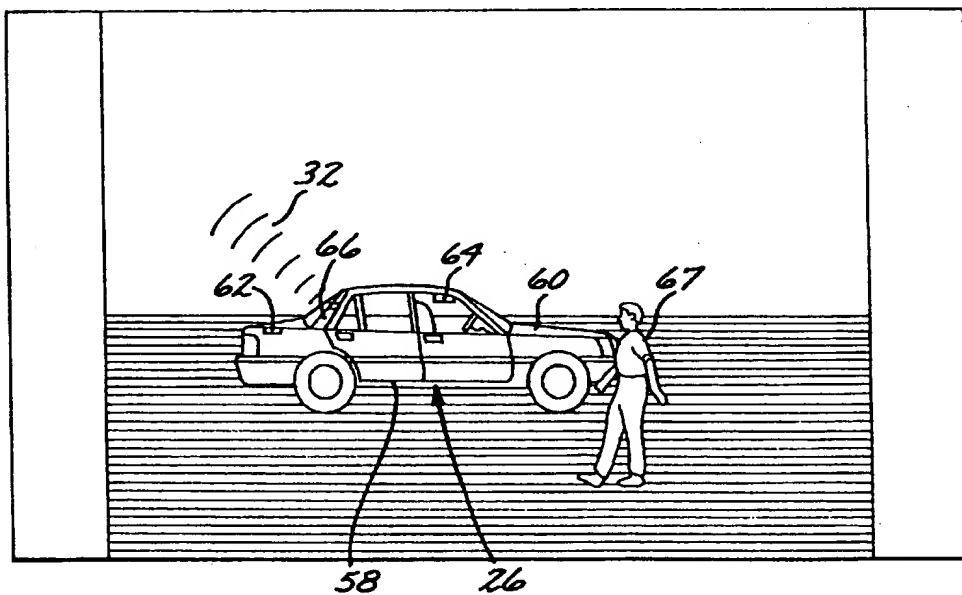


FIG. 6

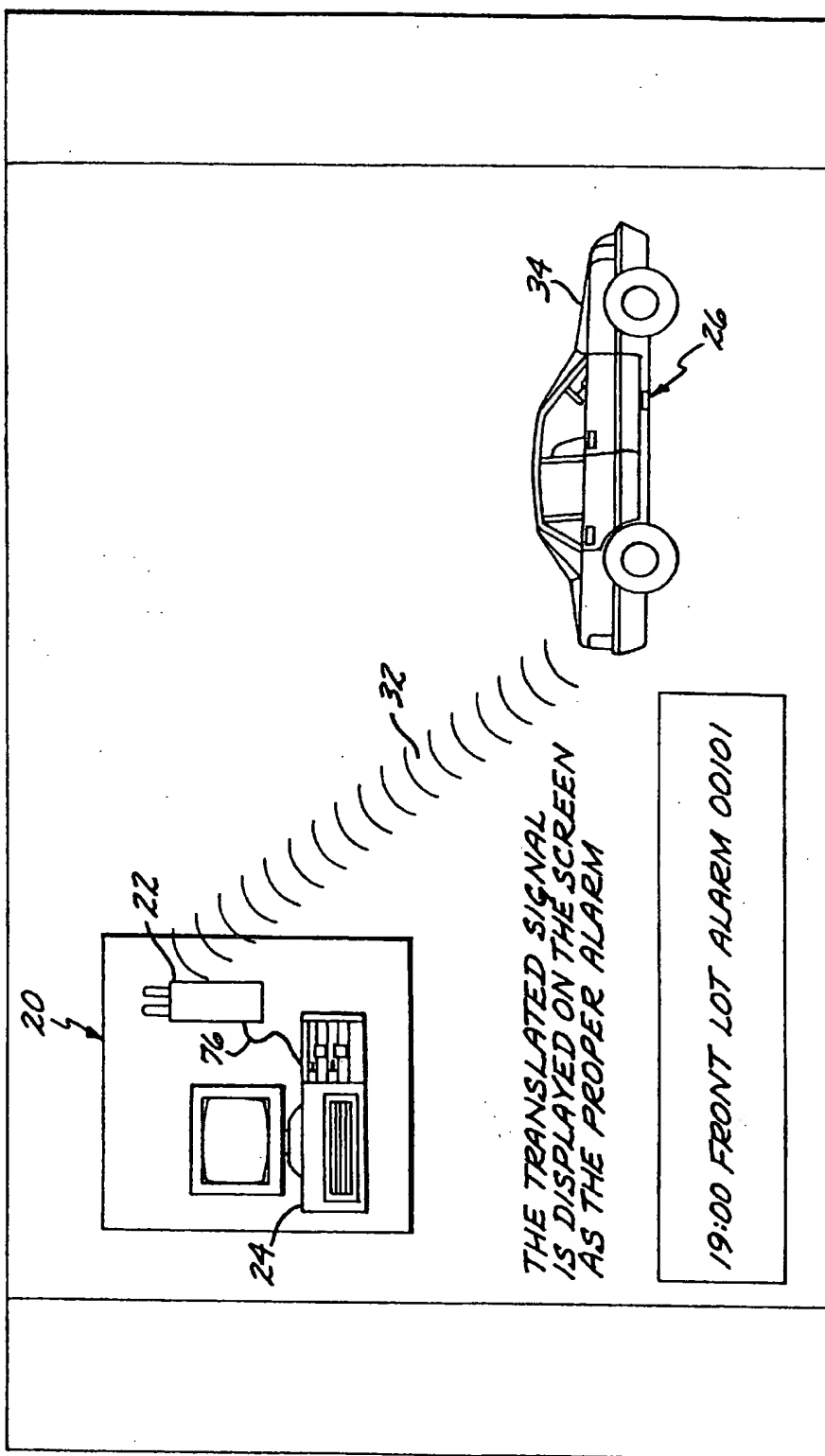


FIG. 5

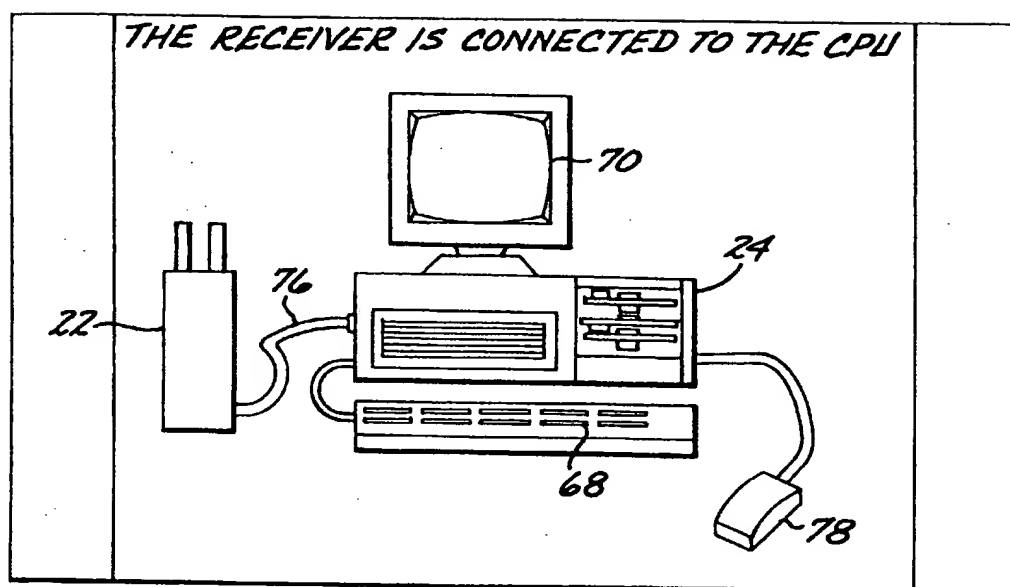
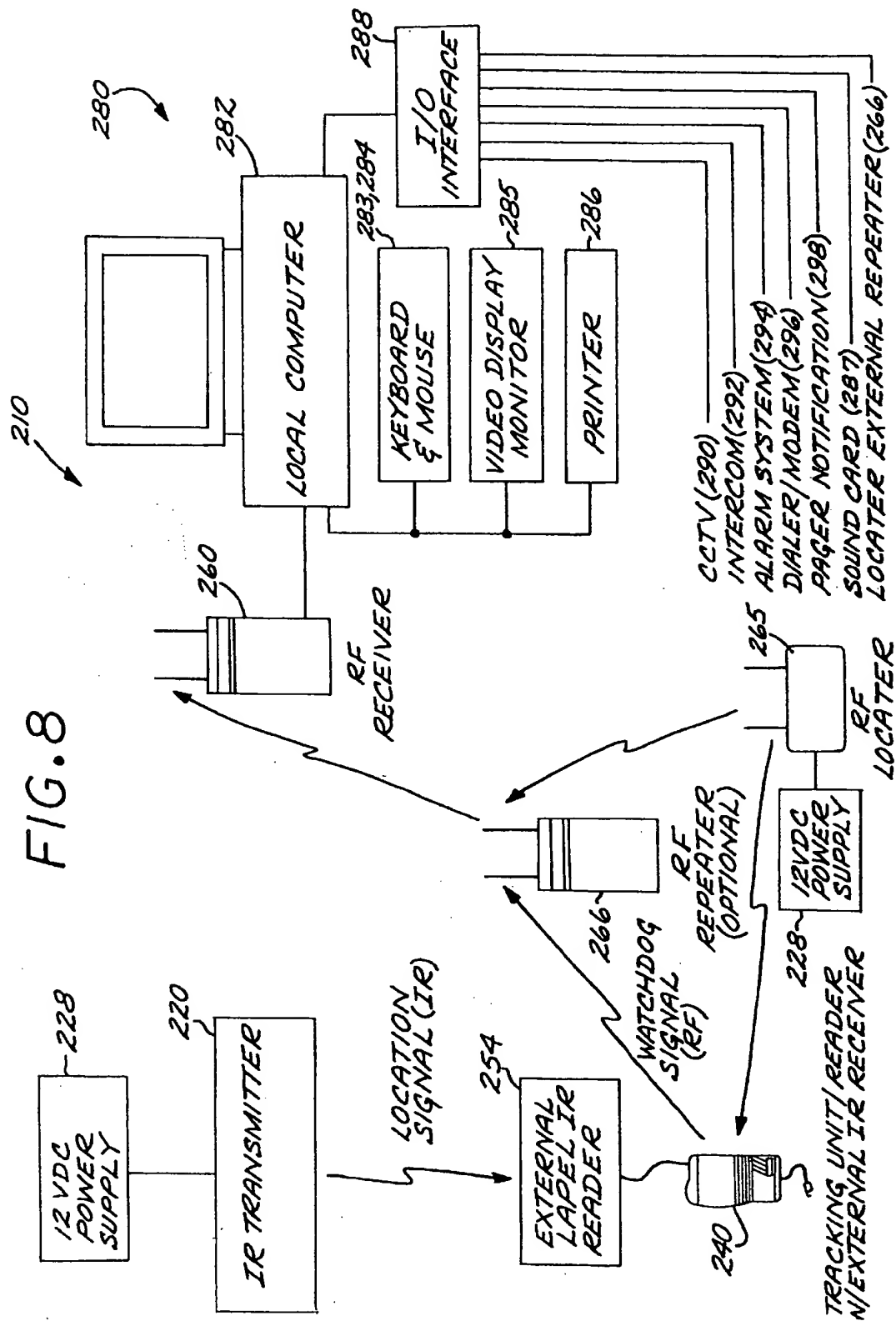


FIG. 7



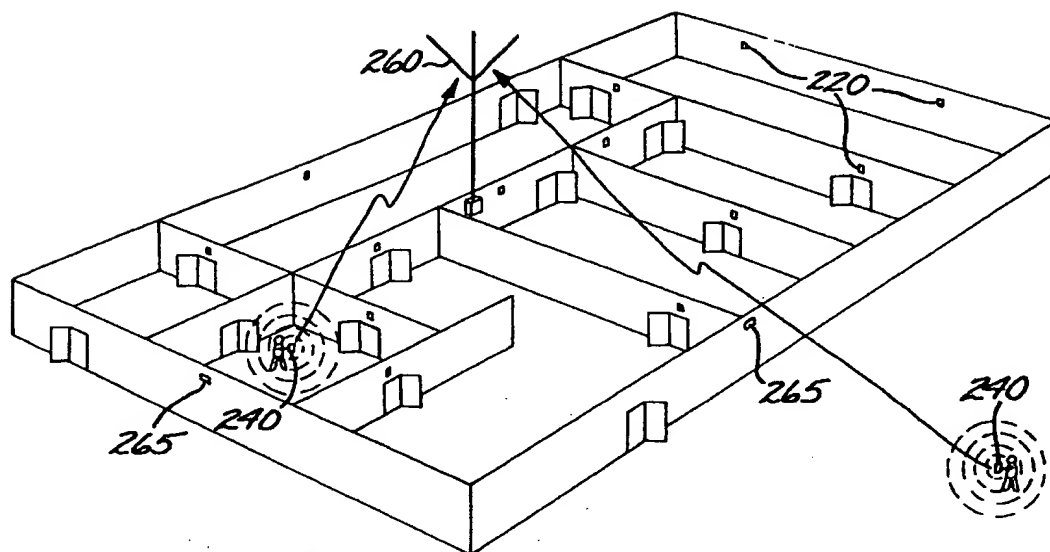


FIG. 9

FIG. 10

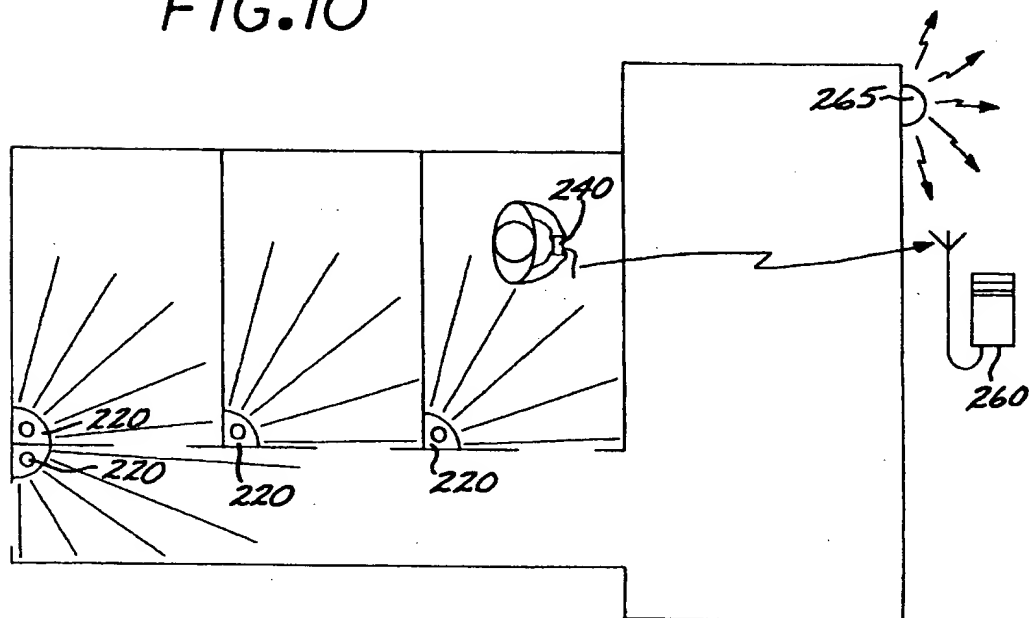


FIG. 11

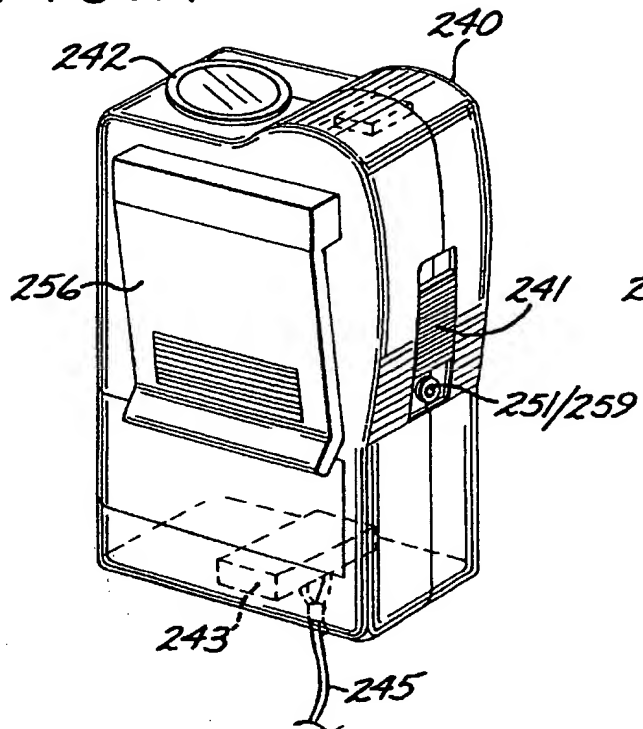


FIG. 12

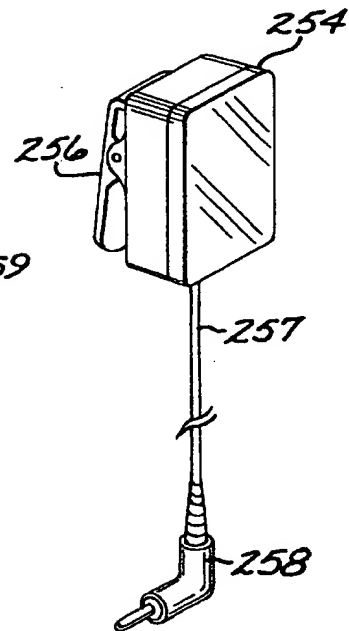
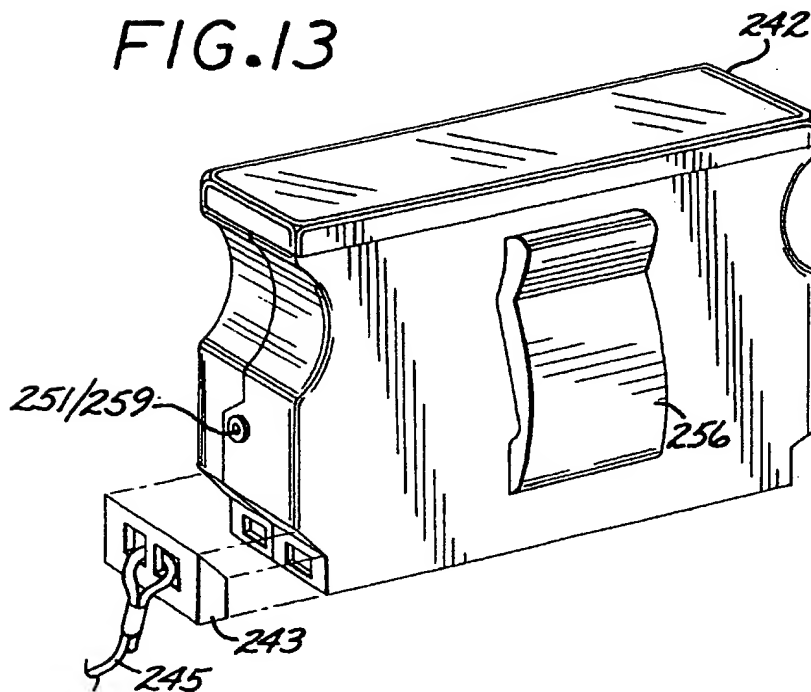


FIG. 13





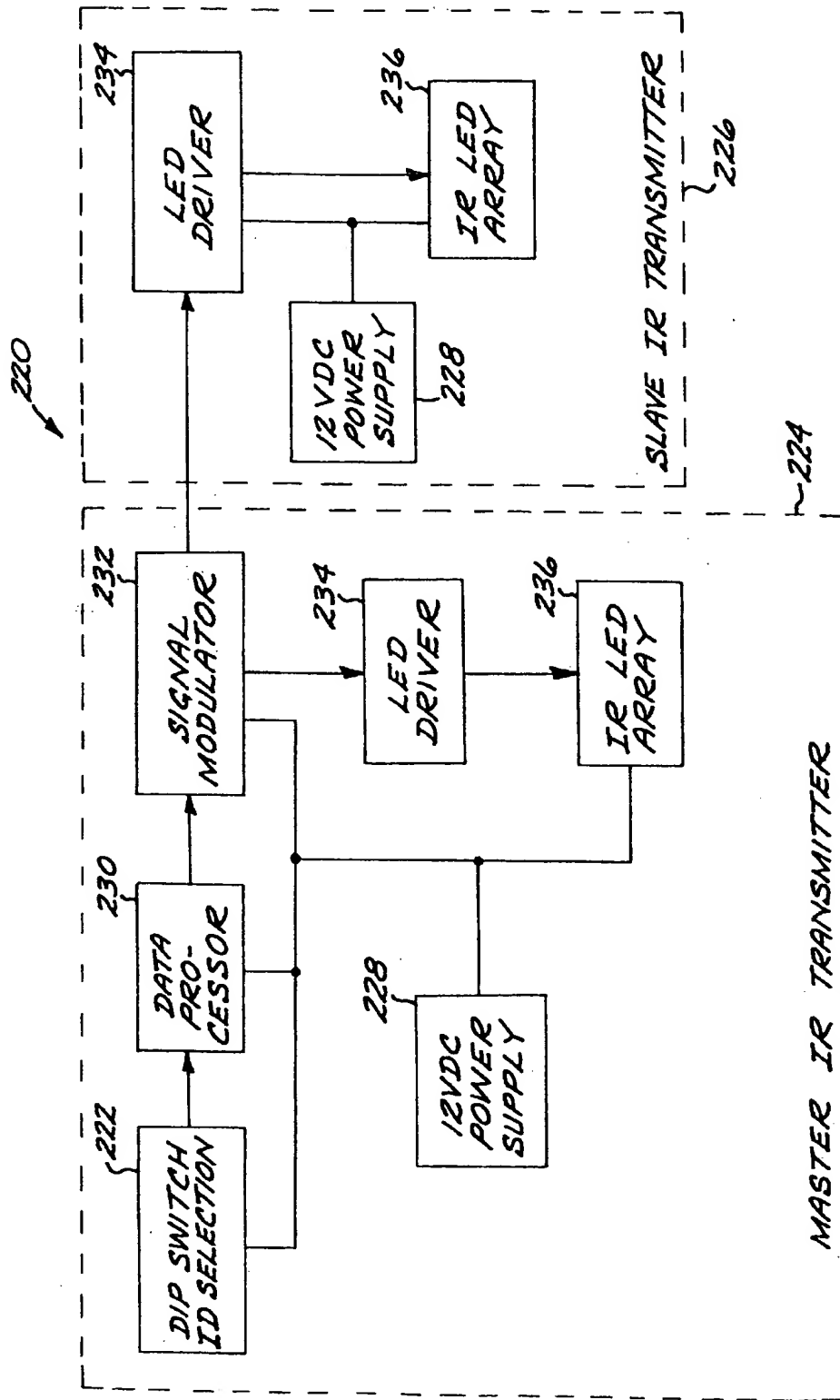


FIG. 14

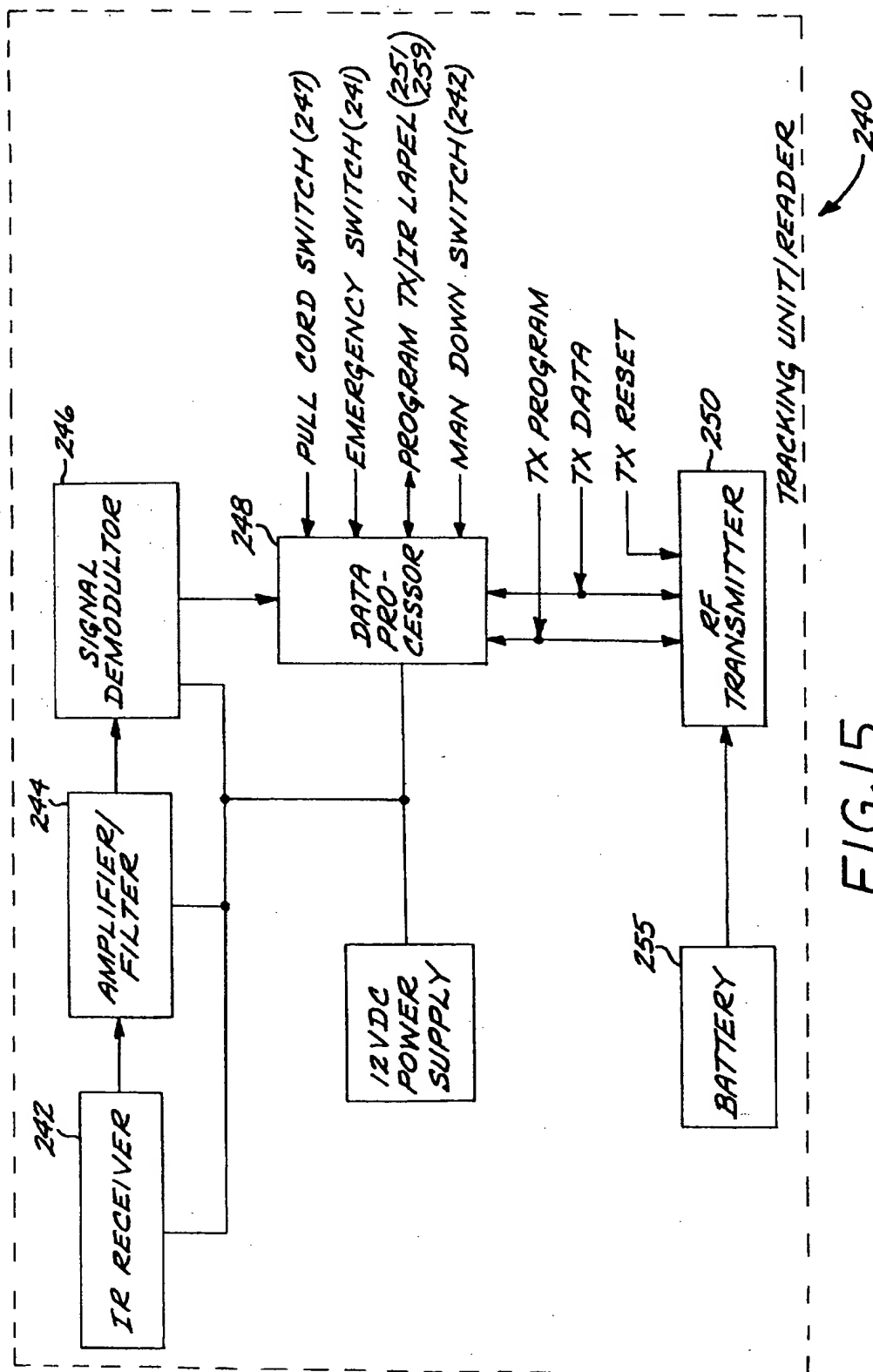


FIG. 15

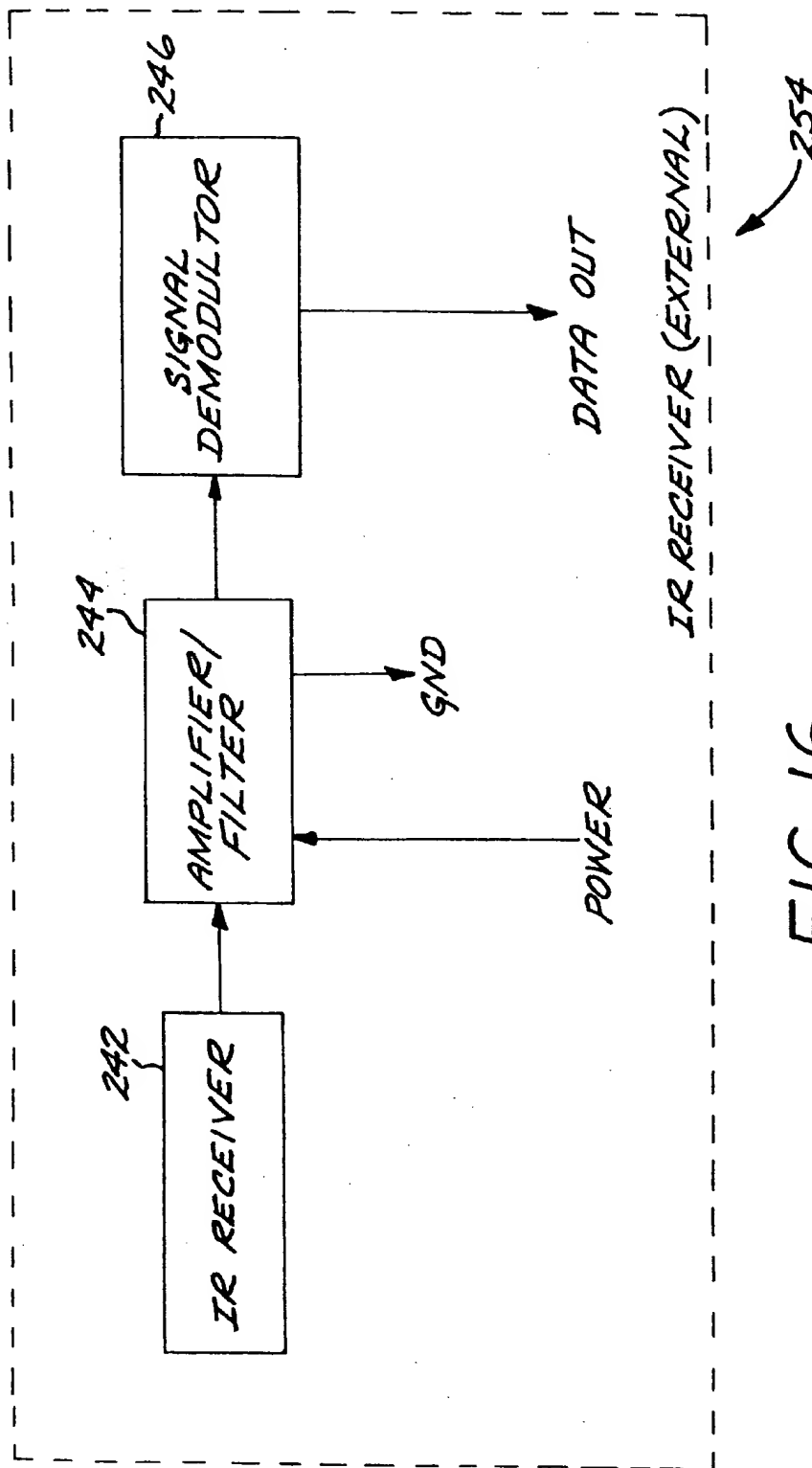


FIG. 16

## PERSONAL DURESS SECURITY SYSTEM

This application is a Continuation of application Ser. No. 08/167,216, filed Dec. 16, 1993, which issued as U.S. Pat. No. 5,708,417 on Jan. 13, 1998. That application, in its entirety, is hereby expressly incorporated herein by reference.

## BACKGROUND OF THE INVENTION

## 1. Field of the Invention

The present invention relates in general to the field of security devices, and, in particular, to a system which may be utilized to track the whereabouts and status of a plurality tracking units carried by persons or items located about a substantial area of interest such as an office building, school campus, hospital, or prison facility, and to communicate data on the status of these persons or items to a central monitoring station.

## 2. Description of the Prior Art

There has long been a need for a security system to provide accurate, meaningful, real time monitoring of persons and objects throughout large areas such as automobile sales lots, office buildings, school campuses, hospitals, and prison facilities. In order for security and loss-prevention professionals to adequately protect the persons and property under their care and supervision, it is necessary for such a security system to indicate the current location of the monitored persons and objects, as well as to set off any one of a number of alarm conditions depending on the need for further investigation and assistance.

Automobile sales lots and congregate care facilities are characterized by an ever-changing inventory arrayed over a relatively large area which must be continually monitored for custodial purposes. Devices have been proposed to monitor unattended automobiles to prevent or discourage theft. Numerous different anti-theft devices have included various bars to lock onto an automobile steering wheel and which in some instances attach to the accelerator pedal.

Other efforts have employed hidden switches to disable the ignition system and shock and motion sensors. Such sensors, upon impulse, actuate an automobile disabling switch and alarm as shown in U.S. Pat. No. 4,990,890. Additionally, it has been proposed to equip vehicles with external radar to sense unauthorized tampering. These systems are relatively expensive and are sometimes ineffective to monitor a large number of vehicles or to make a record of the vehicle subjected to the unauthorized activity. Also, they fail to provide for automatic telecommunication of the alarm to either a central or remote area.

Vehicle security systems have been proposed which included a respective immobilizer and transceiver module in each vehicle. A number of security stations are provided to detect low power signals emitted by vehicles when an unauthorized act is detected. The signals are transmitted to a base station in response to a polling signal therefrom. The compromised vehicle may be immobilized by signals from either the base station or from a security station. A system of this type is disclosed in U.S. Pat. No. 4,990,890.

Other systems have been proposed which include a transmitter in each vehicle to broadcast an emergency signal unique to the vehicle indicative of the nature of the emergency condition. A central station includes a receiver responsive to the signal to operate a transmitter to transmit a disabling signal to a receiver in the vehicle. An alarm sensor can be mounted on each automobile to be monitored. When disturbed, the alarm sensor actuates an automatic dialer to send either a voice or a digital signal identifying the vehicle by a radio telephone to an alarm receiving station. Such systems are shown in U.S. Pat. Nos. 4,067,411 and

4,904,983. This system lacks a self contained transmission capability as it relies on the radio telephone.

Monitoring systems have been proposed which incorporate transmitters mounted on vehicles to be monitored and operative to transmit a watchdog periodic signal to a central receiving station. The transmitted signals become weak and disappear if the vehicles are removed from beyond a predetermined boundary area. The transmitters are responsive to unauthorized tampering to discontinue transmitting thereby generating an alarm. A system of this type is disclosed in U.S. Pat. No. 3,618,067.

In congregate care facilities such as hospitals and nursing homes, monitoring is required so the custodian acting as an overseer can readily check the status of a patient's condition. Further, to be effective, a congregate caretaker must have the capability of quickly responding to any emergency call. In the past, patients have sometimes been provided with manually actuated devices such as pull cords or transmitter buttons to be used in case of emergency. These devices fail to communicate meaningful intelligence to enable the caretaker to determine whether the monitored item has moved from an authorized area or to discern the character of any distress call.

For persons moving about a large geographical area, such as students on a school campus, or security guards patrolling an industrial facility, monitoring systems have been proposed which call for the person to carry a portable tracking unit, such that a person or object may be located in an emergency by locating the tracking unit assigned to that student or guard. Several systems have been proposed that call for the tracking unit to be manually actuated to transmit a distress signal that includes a unique identification code for the particular tracking unit. The distress signal is received by a local receiver, which in turn relays the distress signal, along with a code identifying the particular receiver relaying the distress signal, to a monitoring center where an alarm is triggered and appropriate action may be taken. Such a system is shown in U.S. Pat. No. 5,365,217.

A system utilizing fixed transceivers mounted on street light poles, drawing the necessary electrical power from the local municipal power system that supplies power to the street lights, is shown in U.S. Pat. No. 4,998,095. A system that relies on a plurality of receivers to simultaneously receive the same distress signal so that the location of the tracking unit may be determined by comparing the strength of the distress signal at each receiver is shown in U.S. Pat. No. 5,115,224.

Another proposal, as shown in U.S. Pat. No. 5,572,195, calls for the tracking unit to comprise an infrared transmitter for transmitting an infrared identification code to a plurality of infrared receivers connected to a computer network and located within the area of interest. Finally, yet another proposal, this one calling for local receivers to include processors for processing the received distress signal before passing it on to a central processor which stores the distress signals for periodic determination of tracking unit location, is shown in U.S. Pat. No. 5,455,851.

The above described systems of the prior art, while providing various means for transmitting a distress signal to a central monitoring station, do not provide an adequate means to constantly track the location and motion of a mobile entity in the absence of a manually-actuated distress signal, nor do they provide an adequate alternative to the manual distress signal to detect an emergency situation when the mobile entity is not in a physical condition to manually actuate the distress signal, such as if a person is injured and incapacitated due to a fall. A security system is needed that provides for constant, real time tracking of mobile entities, while being further responsive to a number of alarm conditions to display alarms so assistance may be rendered.

## SUMMARY OF THE INVENTION

The security system of the present invention is characterized by tracking units or readers carried or mounted on mobile units to operatively communicate status signals indicating identity, location, and a number of alarm conditions to a local monitoring station. The tracking units or readers are equipped with receivers to receive location signals transmitted by fixed transmitters located throughout the area to be monitored. Each transmitter transmits a unique location signal. The tracking units are operative to transmit a watchdog signal that includes the last two location signals received, a unique identification signal indicative of the particular tracking unit, and any applicable alarm signals triggered by predetermined conditions to which the tracking unit is also operative to detect. The monitoring station is operative to receive the watchdog signal by way of fixed receivers located throughout the area being monitored and translate the watchdog signal into useful displays.

Other features and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, which illustrate, by way of example, the features of the invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 presents a block diagram of a monitoring system in accordance with the invention;

FIG. 2 is a side view of an automobile with a module included in the system of FIG. 1 mounted thereon;

FIG. 3 is a perspective view in enlarged scale of the module shown in FIG. 1;

FIG. 4 is a top view of a sensor and a transmitter within the module shown in FIG. 3;

FIG. 5 is a perspective view showing the automobile with the module of FIG. 2 transmitting to a local station;

FIG. 6 is a side view of the automobile of FIG. 2 showing the module mounted at various positions thereon;

FIG. 7 is a perspective view of a receiver coupled to a computer at the local station shown in FIG. 1;

FIG. 8 represents a block diagram of a security system in accordance with the preferred embodiment of the present invention;

FIG. 9 is a perspective view of the interior of a building incorporating a security system in accordance with FIG. 8, including tracking units transmitting a watchdog signal to a radio frequency receiver;

FIG. 10 is a top plan view of a corridor of a building incorporating a security system in accordance with FIG. 8, including infrared transmitters transmitting location signals and a tracking unit transmitting a watchdog signal to a radio frequency receiver;

FIG. 11 is a perspective view in enlarged scale of a tracking unit included in the system shown in FIG. 8;

FIG. 12 is a perspective view in enlarged scale of a portable infrared receiver included in the system shown in FIG. 8;

FIG. 13 is a perspective view of a second embodiment of a tracking unit which may be included in the system shown in FIG. 8 and showing a pull cord to generate a pull-cord alert;

FIG. 14 is a block diagram of an infrared transmitter system included in the system of FIG. 8;

FIG. 15 is a block diagram of a tracking unit included in the system of FIG. 8; and

FIG. 16 is a block diagram of a portable infrared receiver included in the system shown in FIG. 8.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As shown in the drawings for purposes of illustration, the invention is directed to a system for monitoring the status and whereabouts of individual mobile units or personnel in a specific area such as a school campus, prison facility, hospital, or industrial facility. Often the number of discrete entities or property units to be monitored is so great that it is not feasible for a single person to effectively monitor all of them.

The present invention is embodied in a system for monitoring a number of mobile units such as automobiles, personnel, or animals. In accordance with the present invention, the system utilizes a tracking unit or reader attached to, or carried by, the mobile unit to be monitored to sense and transmit identity, location, direction of travel, and alarm condition information to a computer monitoring station. The computer is programmed to record the data corresponding to identity, present and previous location, and alarm conditions and display it in a useful manner.

As shown in FIG. 1, the parent duress system of the present invention includes, generally, a local station 20 including a local receiver 22 and a local computer 24 which records and analyzes communications from a plurality of remote modules 26. The modules each include sensors 28 to sense a condition and a transmitter 30 to transmit signals 32 to the local station. The signals transmitted may have any combination of a number of attributes including: shock to the module, tampering, such as an attempt to remove the module from the mobile unit, transportation beyond a predetermined boundary, and low battery in the module.

Referring to FIG. 2, automobiles 34 are typically randomly distributed around an automobile sales lot. The module 26 is attached to each automobile 34 on the lot. The modules 26 each include a housing 36 mounting the respective sensors 28 to activate a transmitter 30 for transmitting from an antenna 38, and a battery 40 as shown in FIGS. 1 and 3. The module housing 36 is constructed of plastic and mounts an annular magnet 42 by means of silicone. The sensors may include a shock sensor 44 (FIG. 1) which detects the presence of a certain level of movement of the car. There may also be a tamper sensor 46 which is activated by unauthorized tampering with the module. The module 26 is magnetically affixed by the magnet 42 to the underside of an automobile 34 as shown in FIG. 2. The module circuit includes a normally open spring loaded switch having an actuation arm which carries an actuation button 48 which protrudes through a bore 50 aligned with the opening in the magnet 42 and to depress to the closed position as a result of this attachment, as shown in FIG. 3. A data port connector 51 (FIG. 3) is formed through the housing and is coupled to the transmitter 30 within the module. An activation switch 52 is formed in said housing and connected in circuit with the internal components of the module to control power to the components.

The transmitter 30 shown in FIG. 4 is responsive to these signals to generate the status signal 32 to be encoded via an encoder 54 (FIG. 1) with a unique identification number associated with the particular module, a battery voltage indicator, a shock flag, and a tamper flag, to be transmitted to the local station 20 by means of the omni-directional antenna 38 (FIG. 1) as shown in FIG. 5. A clock 56, functioning as a proximity signal generator, is coupled with the transmitter to send periodic status signals at regular intervals, for example, every ten minutes. The transmitter power is set relatively low so as to, within a fairly short distance, exceed the range of the signal generated. For automobile lot monitoring, we have selected a power level which provides a signal level of sufficient magnitude to be

5

sensed for so long as the module 26 in the car 34 remains within a distance of about 300 feet from the local station 20, outside this range an alarm is sounded. The components within the module housing are all miniaturized to maintain the module compact.

Signals 32 are transmitted from the module transmitter to the receiver at the local station using the ultra high frequency (UHF) range as shown in FIG. 6. There may be system components interposed between the module and the local station, such as systems for amplification, analysis, or filtration of the transmitted status signals.

Referring to FIG. 1, the local computer 24 is fitted with a keyboard 68, a display 70, and a printer 72. The receiver 22 receives the transmitted signals 32 and converts those signals into digital signals recognizable and readable by a personal computer or a microcomputer. The digital signals are delivered to the local computer by a nine pin serial interface RS-232C connector 76 as shown in FIG. 7. The digital data conforms to recognized RS-232 protocol.

The local computer 24 contains an operating program to monitor in excess of 2,000 mobile units. The computer is programmed to alert in various modes, including prompting an audible alarm, displaying an alarm message on a computer display screen 70 (FIG. 7), printing a hard copy alert on a printer 72 (FIG. 1), or contacting an alpha-numeric pager 80, and alerting a monitoring station 82 (FIG. 1). This provides for response by management personnel, on-site security, off-site guard service, medical attendants, or police.

The monitoring system is controlled using the computer 24 at the local station. The computer 24 is programmed for recording an identification number of each automobile 34 (FIG. 5) to be monitored, an identification number of the module 26 attached to the automobile 34, the price of the automobile, the date of acquisition, whether the automobile is presently in custody, the zone where the automobile is physically located within the lot, a description of the automobile, the serial number of the automobile, ownership information of the automobile, and authorized possessors of the automobile.

The computer 24 is operated by a program to analyze and respond to the signal received from the receiver 22 (FIG. 1). The operating system program functions as a decoder to decode the identification number of the transmitting module as well as shock, tamper, and battery voltage indicator flags from the receiver signal. The operating system also functions as a discriminator for correlating the identification number with an associated module and determining vehicle information from the module identity. The operating system also includes a detector function to detect the absence of a periodically transmitted signal from a module. The computer 24 at the local station thereby decodes alarm flags and detects the absence of such a receiver signal when expected. The local computer 24 (FIG. 1) also monitors the periodic receipt of receiver signals 74 (FIG. 1) from all of the modules attached to automobiles.

The personal security system of the present invention may be embodied in a system adapted primarily to track a person or thing carrying a tracking unit or reader, generally designated as 240 moving about a predetermined area (FIG. 8). The system, generally designated 210 includes, generally, at least one infrared transmitter 220 located within the area to be monitored, one tracking unit or reader 240 per mobile unit to be monitored, at least one radio frequency receiver 260, and a computer monitoring system 280.

The infrared (IR) transmitter 220 generates and broadcasts a unique location code, set by DIP switches 222, via an IR signal of known strength and range. For large areas or rooms for which it is desirable to indicate as a single location, even though the area exceeds the range of the IR

6

signal, the IR transmitter 220 may take the form of one or more slave IR transmitters 226 connected to a master IR transmitter 224 so that a large area, such as an auditorium, may be identified by a single location code. As depicted in FIG. 14, the master IR transmitter 224 operates on a standard 12-volt DC power supply 228. By setting several DIP switches 222, a data processor 230 is programmed to generate a predetermined location signal. A signal modulator 232 converts the digital location signal from the data processor 230 into analog form and sends it to a light-emitting diode (LED) driver 234, which then controls an IR LED array 236 to broadcast the IR location signal. Multiple slave IR transmitters 226, also powered by a standard 12-volt power supply 228, include only the LED driver 234 and IR LED array 236 elements, receiving the analog IR location signal from the master IR transmitter 224. While a 12-volt power supply is supposed here, it should be noted that other power supplies may be used by making appropriate modifications to the circuitry of the IR transmitter 220. The IR transmitters 220 are most effectively located such that the known signal range of each IR transmitter 220 does not overlap with any other IR transmitter 220. As indicated in FIGS. 9 and 10, the IR transmitters 220 may be located on poles, above doors, in a ceiling, or in any other suitable unobtrusive location in a fixed manner to prevent removal or relocation by unauthorized persons. The IR transmitters 220 are suitable for utilizing power from a 12-volt DC power source. In outdoor areas, or in indoor areas with substantial ambient light that interferes with IR signals or where a continuous line of sight is not possible in the room due to partitions of various forms, the IR transmitter 220 may be replaced with or incorporated to operate selectively or continuously in tandem or together with an RF transmitter or locator 265 operating in a substantially similar manner as the IR transmitter 220, but in the radio frequency bandwidth.

A mobile unit moving about the area to be monitored, for instance a security guard patrolling a school campus, will carry a tracking unit or reader 240. The tracking unit or reader 240 (hereinafter referred to only as a reader), as indicated in FIGS. 8-13, is operative to receive the location signals broadcast by the IR transmitters 220. Upon receipt of the location signal, the tracking unit or reader 240 generates a watchdog signal that carries the two most recently received location signals, as well as a unique reader identification code, then transmits the watchdog signal on a radio frequency (RF) signal. The reader 240 is encased in an ABS plastic case, and has dimensions of approximately 10-cm Hx5-cm Wx2.5-cm D, and is powered by a lithium battery. As depicted in FIG. 15, the reader 240 includes an IR receiver 242 for receiving the IR location signal.

Connected to the IR receiver 242 is an electrical amplifier/filter 244 to amplify the IR location signal and increase the signal-to-noise ratio to a useful level. A signal demodulator 246 converts the analog IR location signal to a digital signal suitable for use by the reader's programmable data processor 248. The reader's RF transmitter 250 transmits the watchdog signal using 900 MHz Spread Spectrum Technology via an internal wire antenna 252. The reader 240 further includes an internal programmable data processor 248 which can be programmed with a unique reader identification code and is operative to generate the watchdog signal. The reader 240 also includes a data port 251 for connection by a suitable cable of an external programming device such as a personal computer for programming the data processor 248.

As shown in FIGS. 8 and 12, an external IR receiver 254 may also be used. The external IR receiver 254 includes an external clip 256 for attaching it to an item of outer clothing, such as the lapel of a jacket, or to a carry strap. The external clip 256 may take several forms, including a flexible or

spring-loaded lever, a pin, or a fabric hook and loop fastener such as Velcro. An electrical cable 257 and plug 258 connect the external IR receiver 254 to the reader 240 by means of a plug port 259. The external IR receiver 254 includes an electrical amplifier/filter 244 and a signal demodulator 246. The signal demodulator 246 sends the converted digital IR location signal to the reader's data processor 248 by way of the electrical cable 57. In high ambient light conditions where it is necessary to use the RF transmitters 265 in place of IR transmitters 220 as described above, the IR receiver 242 of the reader 240 may be replaced or incorporated to operate selectively or continuously in tandem or together with a similarly-functional RF receiver.

The internal data processor 248 is also operable to generate a number of auxiliary alarm signals upon detection of certain predetermined alarm conditions. The auxiliary alarm signals are also carried on the watchdog signal to be interpreted by the computer monitor system 280 for display as one of several alerts. A manual emergency switch 241 may be activated to close an internal electrical switch to generate an electrical signal, actuating the transmitter to transmit an immediate panic alarm signal. A pull cord switch assembly 243 is operative to generate a tamper alert when pull cord 245 is pulled, separating the pull cord switch assembly 243 from the rest of the reader 240, triggering the pull cord switch 247, and indicating that someone has attempted to remove the reader 240 from the mobile unit. The pull cord 245 is attached at one end to the pull cord switch assembly 243, and at the other end to the mobile unit itself.

An orientation detector is included, consisting in the preferred embodiment of a mercury tilt switch, normally open, that is operative, when the reader is tilted more than 60 degrees, plus or minus 10 degrees, from its normal upright attitude, to close and trigger a man-down switch 249 and to cause the internal data processor 248 to generate a man-down alarm signal when the reader 240 is rotated in any direction beyond a predetermined tolerance of 15 degrees. Such rotation is indicative that the mobile unit or person carrying the reader 240 has become disabled and has fallen down. In the case of a security guard or other person, the man-down alert allows help to be summoned in the case that the security guard is injured and unable to summon help him/herself. In an alternative embodiment, the data processor 248 can be programmed to delay sending the man-down alarm signal for a predetermined time, and instead flash an LED or trigger an audible buzzer to give the person an opportunity to return the reader 240 to the proper orientation no alarm.

The watchdog signal sent by the reader 240 is received by one or more RF receivers 260, which converts the watchdog signal to a serial data stream to be communicated to the computer monitor system 280 by way of an RS-232 serial cable, the data stream conforming to the RS-232 standard. The RF receiver 260 is powered by a 12 to Volt DC power supply 262, and operates using 900 MHz Spread Spectrum Technology to provide a FCC-certified wireless communications link, receiving the watchdog signal via a 3.5-inch antenna 264. When the readers 240 are to be used in large open areas, wireless RF repeaters (FIG. 8) may optionally be used to greatly extend the transmitting range of the readers 240. The RF repeaters 266 operate on a 12 to 20-volt AC power supply, and operate to receive the watchdog signal from the readers and amplify and retransmit it to the RF receivers 260.

As depicted in FIG. 8, the computer monitor system 280 consists of a local computer 282 fitted with a keyboard 283, mouse 284, video display monitor 285, and a printer 286. The RF receiver 260 receives the watchdog signal and converts it to a serial data stream recognizable and readable by a personal computer or a microcomputer.

In the preferred embodiment, the local computer 282 is an IBM PC-compatible personal computer including an Intel Pentium processor, and capable of running an operating system such as Microsoft (MS) Windows 3.1, MS Windows for Workgroups 3.11, MS Windows 95, MS Windows NT 4.0, or a later version of one of these operating systems that is backward-compatible with software currently operable. The local computer 282 is equipped with at least 16 Megabytes (MB) of random access memory (RAM), though 32 MB is recommended if MS Windows NT is the selected operating system. The local computer 282 also includes a video card for displaying video at a resolution of 1024x768 pixels in at least 16 colors on a 17-inch color video display monitor. An appropriate sound card will allow local alerts to be audibly signaled, and a backup system, for instance, a magnetic tape backup system, will protect system data from loss.

As depicted in FIG. 8, the computer monitor system 280 is connected to an input/output (I/O) interface 288, allowing events registered by the computer monitor system 280 to activate other devices or systems, such as a closed-circuit television (CCTV) system 290 including cameras and monitors, an intercom system 292, or an alarm system 294 including other audible and/or visual alarms such as siren horns, bells, and/or warning lights, or a modem/dialer 296 to contact and send information to another monitoring center, allowing the local computer 282 to be left unattended, calling a central headquarters when alarm conditions are present.

The local computer 282 is equipped with a software program to monitor in excess of 65,000 readers 240, 65,000 IR transmitters 220, and up to eight RF receivers 260, and includes a software database containing all of the attributes of each of these items, including the identification codes associated with each reader and IR transmitter. By comparing the incoming watchdog signal with the values contained in this database, the local computer 282 is operative to display the source of the discerned location signal and reader identification signal. By way of this software program, the local computer is programmed to record the time, according to its internal clock, of receipt of the watchdog signals from the RF receivers 260. The software program records all watchdog signals and alarm signals including emergency manual panic alarms, man-down alarms, pull cord tamper alarms, and alarms related to failure of the reader 240 to detect a location signal or failure to detect a location signal different from the one most recently received by the reader (indicating the mobile unit has become stationary). The software generates a complete log of every transaction that occurs during a monitoring period and provides summary reports of particular actions, such as instances when a watchdog signal is not received, a highlighting of potential injury to mobile units, and notification that certain mobile units have, without prior authorization, been removed from the monitoring area.

In operation, the end user installs the desired number of IR transmitters 220 throughout the area to be monitored, taking care to place the IR transmitters no closer than the effective signal range to ensure that each reader 240 receives only one IR location signal at a time. The DIP switches 222 on each IR transmitter 220 are set to identify each room or section of the area to be monitored with a unique location code. The location codes set for each IR transmitter 220 are also entered into the database of the software program of local computer 282, so the receipt of a particular location code by the local computer 282 will allow an indication of the actual corresponding physical location to be displayed by the monitoring system 280.

A plurality of RF receivers 260 are also installed at locations throughout the monitored area such that the entire

monitored area is covered by the effective reception range of the RF receivers 260. The RF receivers 260 are then connected by cable to the monitoring system 280.

Each person to be tracked in the area to be monitored is issued a reader 240. The database of the software program of local computer 282 is updated to correlate the identity of the person to be tracked with the unique identification of the reader 240, such that when the monitoring system 280 receives a signal from a particular reader 240, the local computer 282 will display the identity of the person carrying that reader 240.

As the person carrying the reader 240 moves about the monitored area, he/she will continually be moving into the signal range of different IR transmitters 220. If the person is wearing heavy clothing, he/she may choose to use the external IR receiver 254 and clip it to his/her outer clothing, while carrying the reader 240 in a pocket, on a belt, or around the neck on a carry strap and plugging the electrical cable 257 into the reader's plug port 259. The IR receiver 242 (internal) or 254 (external) of the reader 240 detects the IR location signal and communicates the last two received location signals to the internal data processor 248. The data processor 248 combines the location signal with its own unique identification signal and periodically causes the reader's RF transmitter 250 to transmit a watchdog signal.

If the person is in apprehension of some harm, he/she may activate a panic alarm by manually actuating the manual emergency switch 241, which causes the data processor 248 to generate a panic alarm signal and combine it with the watchdog signal. If the person should fall, the reader's man-down switch 249 is actuated if the reader 240 tilts more than 60 degrees, plus or minus 10 degrees, from the normal upright position and isn't righted within a predetermined time. When actuated, the man-down switch 249 causes the data processor to generate a man-down alarm signal, which is combined with the watchdog signal transmitted by RF transmitter 250. A pull-cord assembly 243 is attached at one end to the reader 240 and at the other end to the person carrying the reader. If the reader 240 is forcibly removed from the person, for instance in case of an attack by a violent perpetrator, the pull-cord switch 247 is actuated, causing the data processor to generate a pull-cord alarm signal, which is combined with the watchdog signal.

The watchdog signal transmitted by the reader 240 is received by the closest RF receiver 260 and communicated to the local computer 282 of the monitor system 280. The software program of the local computer 282 reads the IR transmitter or RF locator location signals, reader identification signals, and any alarm signals, and compares the signals to its database to generate one or more displays that indicate the identity of the person carrying the particular reader 240, the location of the IR transmitter 220 closest to the person, the location of the IR transmitter 220 most recently previously encountered by the reader 240, and any alarm conditions indicated by the alarm signals. The incoming signals may also cause the monitoring system 280 to produce an audible alarm, communicate with another monitoring location by means of the dialer/modem 296, activate a CCTV system 290 to visually monitor the location, or activate an intercom system 292, so verbal communication with the person being tracked may be initiated.

While multiple particular forms of the present invention have been illustrated and described, it will also be apparent that various modifications can be made without departing from the spirit and scope of the invention.

What is claimed is:

1. A security apparatus for monitoring a condition of a mobile unit to be located in a predetermined area and comprising:

a plurality of location transmitters to be spaced a selected distance apart within said predetermined area and

operative to generate and transmit respective location signals identifying the respective location transmitters; at least one portable reader to be carried on said mobile unit and including a portable receiver for receiving said location signals and a signal generator responsive to said location signals to generate a spread spectrum watchdog signal corresponding to the respective location signals and indicative of the particular said portable reader, said portable reader also including a portable transmitter for transmitting said spread spectrum watchdog signal;

at least one stationary receiver responsive to said watchdog signal to despread and demodulate said watchdog signal to generate a control signal indicative of said watchdog signal; and

a monitor for coupling with said stationary receiver and responsive to said control signal to generate a readout indicative of the location transmitter generating the respective location signals.

2. A security apparatus according to claim 1 for connection with a selected power source and wherein:

said location transmitters are adapted for connection with said selected power source and are operative to generate respective location signals having a predetermined strength at a predetermined distance from the respective said location transmitters; and

said portable receivers being operative to, upon detecting said location signals at or above said predetermined strength, generate said watchdog signals.

3. A security apparatus according to claim 1, wherein: said monitor is operative to generate said readout signal as a visual signal or audio signal.

4. A security apparatus according to claim 1, wherein: said monitor includes a computer.

5. A security apparatus according to claim 1, wherein: said portable readers include respective auxiliary inputs operative to generate auxiliary signals to be carried on the respective watchdog signals to produce respective auxiliary watchdog signals;

said monitor includes a receiver responsive to said auxiliary watchdog signals to generate corresponding auxiliary electrical signals; and

said monitor includes an auxiliary alert responsive to said auxiliary electrical signals to generate an alert.

6. A security apparatus according to claim 1, wherein: said portable reader includes a detector responsive to the absence of said location signal to generate and transmit a missing-unit alarm signal;

said receiver includes means responsive to said missing-unit alarm signal to generate a missing-unit alarm electrical signal; and

said monitor includes an alarm responsive to said alarm electrical signal to generate a perceptible alarm.

7. A security apparatus according to claim 1, wherein: said portable reader includes a plurality of components and a tamper circuit connected with said components and responsive to shifting of any one of said components to generate a portable reader tamper signal; and said receiver is responsive to said portable reader tamper signal to generate a portable reader tamper electrical signal; and

said monitor is responsive to said electrical signal to generate a tamper alarm.

8. A security apparatus according to claim 5 wherein: said auxiliary inputs include a manual actuation button which may be activated to close an internal switch to



11

generate an electrical signal, actuating the transmitter to transmit an immediate panic alarm signal.

9. A security apparatus according to claim 1 wherein:

said monitor includes a memory for detecting watchdog signals corresponding to each of said location transmitters and a detector responsive to the absence of watchdog signals from at least one of said location transmitters to generate an electrical loss signal, and a loss alert responsive to said loss signal to generate a loss alert alarm.

10. A security apparatus according to claim 1 wherein:

said monitor includes a detector for detecting the presence of a watchdog signal corresponding with each of said transmitters and operative in response to the absence of a watchdog signal corresponding with any one of said transmitters to generate a location alert electrical signal, and a loss alert responsive to said electrical signal to generate a loss alarm.

11. A security apparatus according to claim 1 wherein:

said portable readers include a detector for detecting the respective actual attitude and orientation of the respective said portable readers relative to respective reference attitudes and orientations to, upon detection of said actual attitude and orientation differing from said reference attitude and orientation, generate respective man-down electrical signals if said attitude and orientation deviates from said reference by more than a predetermined amount; and

said monitor is responsive to said man-down electrical signal to generate a man-down alarm.

12. A security apparatus as set forth in claim 1 wherein:

said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

13. A security system for monitoring and tracking the movement and condition of a plurality of mobile remote units located within a predetermined area of interest, comprising:

a plurality of fixed infrared transmitters located at selected locations throughout said predetermined area of interest, each of said fixed infrared transmitters generating and transmitting a unique location signal of a predetermined signal strength and signal range such that said fixed infrared transmitters may be arranged in a spaced apart manner at a distance equal to approximately twice said known signal range;

at least one portable reader, including a portable infrared receiver responsive to said location signals from said fixed infrared transmitters, attached to each of said mobile remote units and operative to generate and transmit a spread spectrum watchdog signal, said watchdog signal carrying said unique location signal as well as a unique portable reader identification signal;

at least one fixed receiver for receipt, despread and demodulation of said watchdog signal and located such that said watchdog signals may be detected throughout entire said predetermined area of interest; and

a monitor system connected with said fixed receiver and responsive to said watchdog signal to display identification and location information.

14. The security system of claim 13, further including:

at least one radio frequency repeater to receive said watchdog signal and retransmit it to said fixed receivers.

15. The security system of claim 13, wherein:

said portable reader includes an auxiliary alarm signal generator for generating and sending auxiliary alarm signals on the respective said watchdog signals; and

12

said monitor system is further responsive to said auxiliary alarm signals to monitor and report respective said auxiliary alarm signals received.

16. The security system of claim 15, wherein:

said portable reader includes an exterior casing;

said portable receiver is located outside said exterior casing and is connected to said portable reader by a suitable electrical cable and includes a clip for releasable attachment to outer clothing; and

said portable reader includes a clip for releasably fastening said portable reader to a piece of clothing or hanger.

17. The security system of claim 15, that includes:

a flexible tether attaching said portable receiver to said portable reader such that said portable receiver may be manipulated about relative to said portable reader.

18. The security system of claim 15, wherein:

said portable reader is responsive to the absence of any of said location signals to cause said auxiliary alarm signal generator to generate a location loss auxiliary alarm signal to be carried on said watchdog signal; and said monitor system is responsive to said location loss auxiliary alarm signal to generate a location loss alert.

19. The security system of claim 15, wherein:

said portable reader includes a manual switch to cause said auxiliary alarm signal generator to generate a manual panic auxiliary alarm signal to be carried on said watchdog signal; and

said monitor system is responsive to said manual panic auxiliary alarm signal to generate a manual panic alert.

20. The security system of claim 15, wherein:

said portable reader includes a detachable pull-cord switch assembly and a pull-cord switch responsive to disconnection of said pull-cord switch assembly to cause said auxiliary alarm signal generator to generate a pull-cord auxiliary alarm signal to be carried on said watchdog signal; and

said monitor system is responsive to said pull-cord auxiliary alarm signal to generate a pull-cord alert.

21. The security system of claim 15, wherein:

said portable reader includes a detector to detect change in attitude or orientation relative to a preselected reference and is responsive to a predetermined magnitude of said change to cause said auxiliary alarm signal generator to generate a man-down auxiliary alarm signal to be carried on said watchdog signal; and

said monitor system is responsive to said man-down auxiliary alarm signal to generate a man-down alert.

22. The security system of claim 13, wherein:

said monitor system includes a computer.

23. The security system of claim 22, wherein:

said computer includes an input interface to read said watchdog signal and a software control program responsive to said watchdog signal, a software database of all said location signals, portable reader identification signals, and auxiliary alarm signals, and an output interface operative to direct said signals to a display device to display indices corresponding with the respective said signals.

24. A security apparatus as set forth in claim 13 wherein:

said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

25. A security apparatus as set forth in claim 13 wherein:

said location transmitters and portable receivers may be replaced or incorporated to operate selectively or con-

13

tinuously in tandem using infrared and RF to be operative indoors in high ambient light conditions and outdoors.

26. A personal duress security system for monitoring the location, motion, and status of each of a plurality of persons located within a preselected area, and comprising:

a plurality of fixed infrared transmitters installed at various selected locations throughout said preselected area and operative to generate respective infrared signals unique to each of said infrared transmitters;

a plurality of portable personal tracking units bearing respective identification indicia and including respective infrared receivers, internal data processors, and radio frequency transmitters connected together in an electrical circuit, said infrared receivers operative to detect the respective said infrared signals and operative in response thereto to generate an actuation signal and to communicate said actuation signal to said data processor, said data processor being responsive to said actuation signals and operative to periodically generate a spread spectrum watchdog signal including last two received said actuation signals corresponding with the respective infrared signals and carrying as a component, a tracking unit identification signal, and any of a plurality of alarm signals in response to a selected plurality of alarm conditions and direct said watchdog signal to said radio frequency transmitter, said radio frequency transmitter being operative to periodically broadcast said watchdog signal;

a computer control system responsive to said watchdog signal and operative to distinguish said location signal, said identification signal, and said alarm signals from each other within said watchdog signal and consult a database of known values for said signals such that the location of the last two infrared transmitters, the identity of the person associated with said tracking unit, and the presence of any of said plurality of alarm conditions causing one or more of said plurality of alarm signals may be displayed in a convenient manner on a computer monitor and/or a computer printer; and

at least one radio frequency receiver connected to said computer control system and operative to receive, despread and demodulate said watchdog signal and carry it to said computer control system.

27. The personal duress security system of claim 26, further including:

at least one radio frequency repeater operative to detect said watchdog signal and retransmit it to said radio frequency receivers.

28. The personal duress security system of claim 26, wherein:

said infrared receiver is flexibly connected to the exterior of said tracking unit such that said tracking unit may be carried by hand or in a pocket and said infrared receiver may be releasably attached to an article of outer clothing.

29. The personal duress security system of claim 26, wherein:

said tracking unit includes a manual switch operative to generate a panic alarm signal; and

said computer control system is responsive to said panic alarm signals to display a panic alert.

30. The personal duress security system of claim 29, wherein:

said internal data processor includes a detector operative to determine that it is not receiving any said location signal and generate a second said one of said alarm signals; and

14

said computer control system is responsive to said second alarm signal to display an out-of-area alert.

31. The personal duress security system of claim 29, wherein:

said tracking units include a respective pull-cord switch operative to generate respective pull-cord alarm signals and respective detachable pull-cord switch assemblies operative upon pulling thereon to actuate the respective pull-cord switches; and

said computer control system is responsive to said pull-cord alarm signals to display a pull-cord alert.

32. The personal duress security system of claim 29, wherein:

said internal data processor includes an orientation detector to detect any change in attitude or orientation of said tracking unit relative to a preselected reference and generate a man-down alarm signals; and

said computer control system is responsive to said man-down alarm signal to display a man-down alert.

33. The personal duress security system of claim 26, further including:

an alarm system coupled with said computer control system and responsive to said alarm signals and operative to generate an audible alert.

34. A security apparatus as set forth in claim 26 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

35. A portable security apparatus for use with a security system for monitoring the location, movement, and status of at least one mobile unit to be located in a predetermined area including at least one infrared transmitter to be located at a selected location within said predetermined area and operative to transmit an infrared location signal indicative of said infrared transmitter, said apparatus comprising:

a radio frequency transmitter operative to generate a spread spectrum watchdog signal;

at least one radio frequency receiver located within said predetermined area and operative to receive and despread and demodulate said watchdog signal and transmit it to a monitor system, said monitor system operative to convert said watchdog signal to a useful display, said apparatus comprising:

an infrared receiver operative to receive said location signal; and

a signal generator operative to generate an identification signal unique to said apparatus, said identification signal being carried on said watchdog signal, said watchdog signal including said location signal.

36. The portable security apparatus of claim 35, wherein: said infrared receiver includes a clip for releasable attachment to an article of clothing and is flexibly attached to the exterior of said apparatus by a suitable electrical cable.

37. The portable security apparatus of claim 35, wherein: said signal generator includes a memory operative to store last two said location signals detected, said signal generator also operative to include said last two location signals with said watchdog signal.

38. The portable security apparatus of claim 35, further including:

a manual switch operative to cause said signal generator to generate a manual panic alarm signal to be included in said watchdog signal.

15

39. The portable security apparatus of claim 35, further including:

an external housing encasing said apparatus; and  
a data port connector formed through said housing and operative to allow an external programming device to connect to said signal generator and memory to permit programming thereof.

40. A security apparatus as set forth in claim 35 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

41. A security apparatus as set forth in claim 35 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

42. A security apparatus for monitoring a condition of a mobile unit to be located in a predetermined area and comprising:

a plurality of location transmitters to be spaced a selected distance apart within said predetermined area and operative to generate and transmit respective location signals identifying the respective location transmitters;  
at least one portable reader to be carried on said mobile unit and including a portable receiver for receiving said location signals and responsive to said location signals to generate a spread spectrum watchdog signal corresponding to the respective location signals and also including a portable transmitter for transmitting said watchdog signal and further including respective auxiliary inputs operative to generate auxiliary signals to be carried on said watchdog signal to produce respective auxiliary watchdog signals;

at least one stationary receiver responsive to despread and demodulate said watchdog signal to generate a control signal indicative of said watchdog signal; and

a monitor for coupling with said stationary receiver and responsive to said control signal to generate a readout indicative of the location transmitter generating the respective location signals and including a receiver responsive to said auxiliary watchdog signals to generate corresponding auxiliary electrical signals; and  
said monitor includes an auxiliary alert responsive to said auxiliary electrical signals to generate an alert.

43. A security apparatus as set forth in claim 42 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

44. A security system for monitoring and tracking the movement and condition of a plurality of mobile remote units located within a predetermined area of interest, comprising:

a plurality of fixed transmitters located at selected locations throughout said predetermined area of interest, each of said transmitters generating and transmitting a unique location signal of a predetermined signal strength and signal range such that said fixed transmitters may be arranged in a spaced apart manner at a distance equal to approximately twice said known signal range;

at least one portable reader, including a portable receiver responsive to said location signals from said fixed transmitters, attached to each of said mobile remote units and operative to generate and transmit a spread spectrum watchdog signal, said watchdog signal carrying said unique location signal as well as a unique portable reader identification signal, said portable

16

reader further including an auxiliary alarm signal generator operative to generate and send auxiliary alarm signals on the watchdog signal;

at least one fixed receiver for receipt, despread and demodulation of said watchdog signal and located such that said watchdog signals may be detected throughout entire said predetermined area of interest; and

a monitor system connected with said fixed receiver and responsive to said watchdog signal to display identification and location information as well as to monitor and report said auxiliary alarm signals received.

45. A security apparatus as set forth in claim 44 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

46. A security system for monitoring and tracking the movement and condition of a plurality of mobile remote units located within a predetermined area of interest, comprising:

a plurality of fixed transmitters located at selected locations throughout said predetermined area of interest, each of said transmitters generating and transmitting a unique location signal of a predetermined signal strength and signal range such that said fixed transmitters may be arranged in a spaced apart manner at a distance equal to approximately twice said known signal range;

at least one portable reader, including a portable receiver responsive to said location signals from said fixed transmitters, attached to each of said mobile remote units and operative to generate and transmit a spread spectrum watchdog signal, said watchdog signal carrying said unique location signal as well as a unique portable reader identification signal;

at least one fixed receiver for receipt, despread and demodulation of said watchdog signal and located such that said watchdog signals may be detected throughout entire said predetermined area of interest; and

a monitor system connected with said fixed receiver and responsive to said watchdog signal to display identification and location information, said monitor system including a computer, said computer including an input interface to read said watchdog signal and a software control program responsive to said watchdog signal, a software database of all said location signals, portable reader identification signals, and auxiliary alarm signals, and an output interface operative to direct said signals to a display device to display indices corresponding with the respective said signals.

47. A security apparatus as set forth in claim 46 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

48. A personal duress security system for monitoring the location, motion, and status of each of a plurality of persons located within a preselected area, and comprising:

a plurality of fixed infrared transmitters installed at various selected locations throughout said preselected area and operative to generate respective infrared signals unique to each of said infrared transmitters;

a plurality of portable personal tracking units bearing respective identification indicia and including respective infrared receivers, internal data processors, and radio frequency transmitters connected together in an electrical circuit, said infrared receivers operative to detect the respective said infrared signals and operative

17

in response thereto to generate an actuation signal and to communicate said actuation signal to said data processor, said data processor being responsive to said actuation signals and operative to periodically generate a spread spectrum watchdog signal including last two received said actuation signals corresponding with the respective infrared signals and carrying as a component, a tracking unit identification signal, and any of a plurality of alarm signals in response to a selected plurality of alarm conditions and direct said watchdog signal to said radio frequency transmitter, said radio frequency transmitter being operative to periodically broadcast said watchdog signal;

said tracking unit further includes a manual switch operative to generate a panic alarm signal;

said tracking unit further includes an orientation detector to detect any change in attitude or orientation of said tracking unit relative to a preselected reference and generate a man-down alarm signal;

a computer control system responsive to said watchdog signal and operative to distinguish said location signal, said identification signal, and said alarm signals from each other within said watchdog signal and consult a database of known values for said signals such that the location of the last two infrared transmitters, the identity of the person associated with said tracking unit, and the presence of any of said plurality of alarm conditions causing one or more of said plurality of alarm signals may be displayed in a convenient manner on a computer monitor and/or a computer printer; said computer control system further responsive to said panic alarm signal to display a panic alert and also responsive to said man-down alarm signal to display a man-down alert; and

at least one radio frequency receiver connected to said computer control system and operative to receive, despread and demodulate said watchdog signal and carry it to said computer control system.

49. A security apparatus as set forth in claim 48 wherein: said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

50. A monitoring system for identifying and tracking at least one selected mobile unit present within a predetermined area, comprising:

at least one fixed infrared location transmitter located within said predetermined area and including a location signal generator operative to generate a unique location signal, said location transmitter operative to broadcast said location signal;

18

a portable reader carried on each of said at least one selected mobile units and including an infrared receiver operative to receive said location signal, a signal processor electronically connected to said infrared receiver and operative to combine said location signal with an identification signal unique to each of said portable readers and to generate a combined spread spectrum watchdog signal, and a radio frequency transmitter electronically connected to said signal processor and operative to broadcast said watchdog signal;

at least one fixed radio frequency receiver operative to receive, despread and demodulate said watchdog signal and relay it to a central monitoring station, said central monitoring station responsive to said watchdog signal and operative to decode said combined watchdog signal, determine location and identify of said at least one selected mobile unit, and display information relating to said location and identity in a useful format.

51. The monitoring system of claim 50, wherein:

said portable reader further includes at least one sensor responsive to a predetermined condition, said sensor being electronically connected to said signal processor and operative to generate an alarm signal in response to detection of said predetermined condition and send said alarm signal to said signal processor for combination into said combined watchdog signal; and

said central monitoring station is further operative to also determine from said alarm signal within said watchdog signal the existence of said predetermined condition and display information related to existence of said predetermined condition.

52. The monitoring system of claim 50, wherein:

said portable reader further includes a memory operative to store the last previously received said location signal, said memory electronically connected to said signal processor, said signal processor further combining said last previously received location signal into said combined watchdog signal; and

said central monitoring station is further operative to determine from said last previously received location signal within said watchdog signal a previous location of said portable reader and display information related to said previous location.

53. A security apparatus as set forth in claim 50 wherein:

said signal generator is responsive to said location signals to generate a 900 MHz spread spectrum watchdog signal.

\* \* \* \* \*

# United States Patent [19]

Bethards

[11] Patent Number: 5,040,212

[45] Date of Patent: Aug. 13, 1991

[54] METHODS AND APPARATUS FOR  
PROGRAMMING DEVICES TO RECOGNIZE  
VOICE COMMANDS

[75] Inventor: Charles Bethards, Colleyville, Tex.

[73] Assignee: Motorola, Inc., Schaumburg, Ill.

[21] Appl. No.: 501,384

[22] Filed: Mar. 19, 1990

## Related U.S. Application Data

[63] Continuation of Ser. No. 213,803, Jun. 30, 1988, abandoned.

[51] Int. Cl.<sup>5</sup> ..... G01L 5/00

[52] U.S. Cl. .... 381/41; 364/513.5

[58] Field of Search ..... 381/41-46,  
381/110; 364/513.5; 367/198

## References Cited

### U.S. PATENT DOCUMENTS

4,233,685 11/1980 Taylor ..... 455/151  
4,422,071 12/1983 De Graaf ..... 340/825.44  
4,462,080 7/1984 Johnstone et al. .... 364/513.5  
4,525,865 1/1985 Mears ..... 455/186  
4,593,155 6/1986 Hawkins ..... 179/2 EA  
4,720,802 1/1988 Damoulakis ..... 381/43

4,731,811 3/1988 Dubus ..... 379/58  
4,737,976 4/1988 Borth ..... 381/46  
4,776,016 10/1988 Hansen ..... 381/42  
4,797,924 1/1989 Schnars et al. .... 381/43  
4,797,929 1/1989 Gerson et al. .... 381/43  
4,984,295 1/1991 Engstrom et al. .... 455/186

## FOREIGN PATENT DOCUMENTS

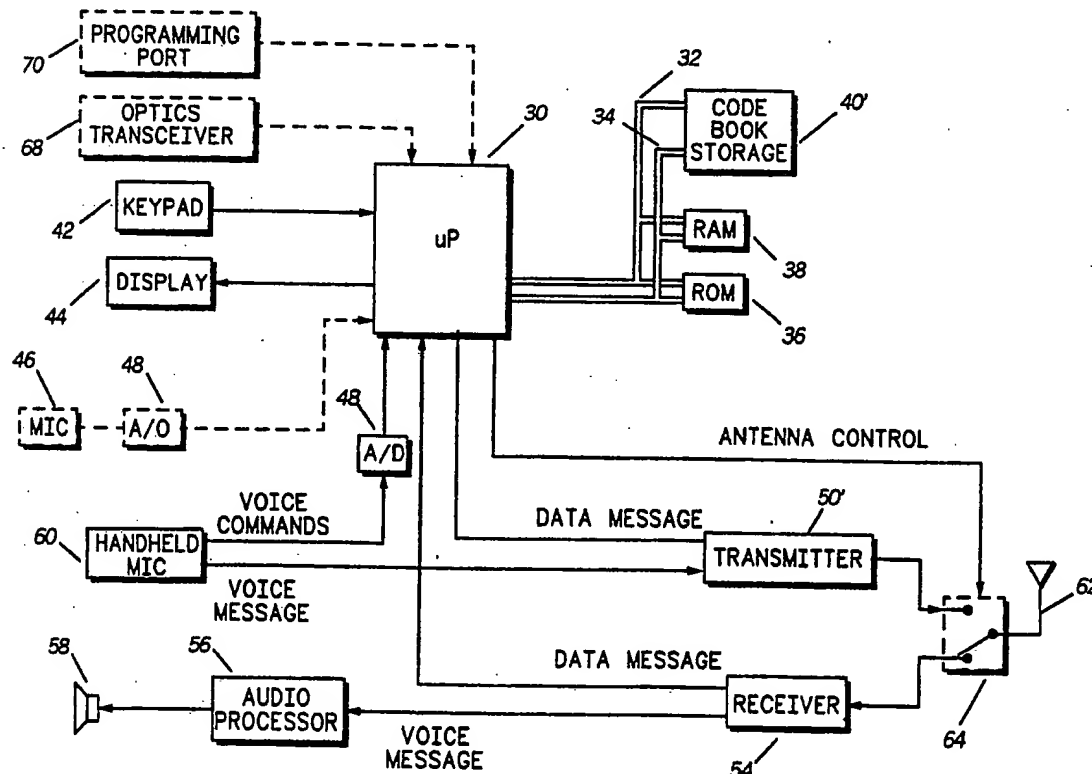
0041195A1 12/1981 European Pat. Off. .  
2016768A 9/1979 United Kingdom .

Primary Examiner—Emanuel S. Kemeny  
Attorney, Agent, or Firm—Thomas G. Berry

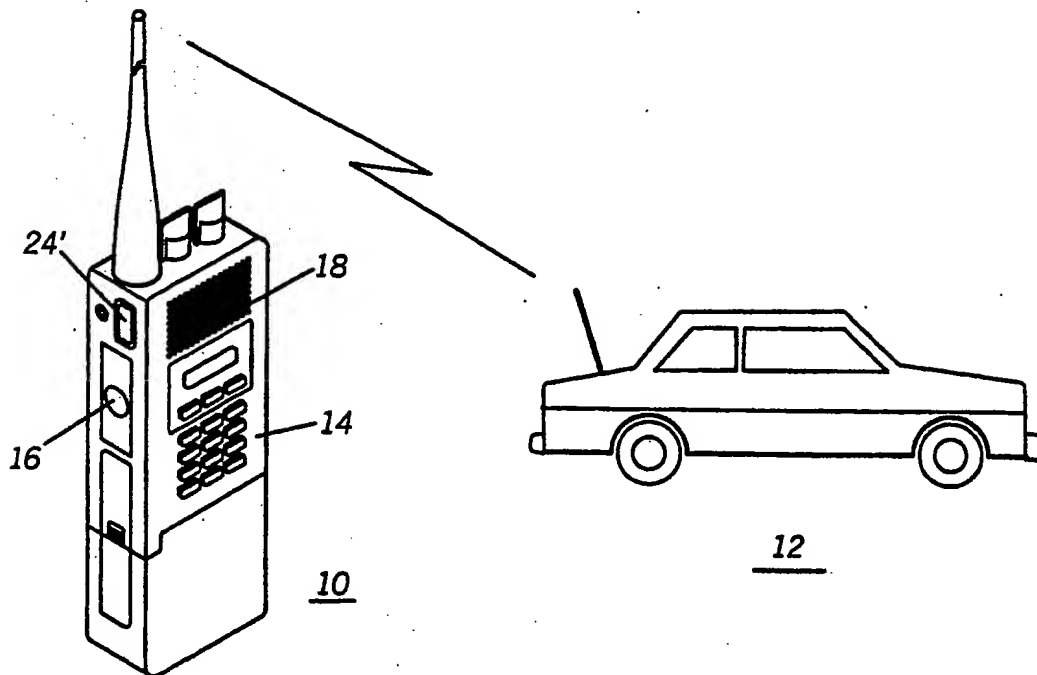
## [57] ABSTRACT

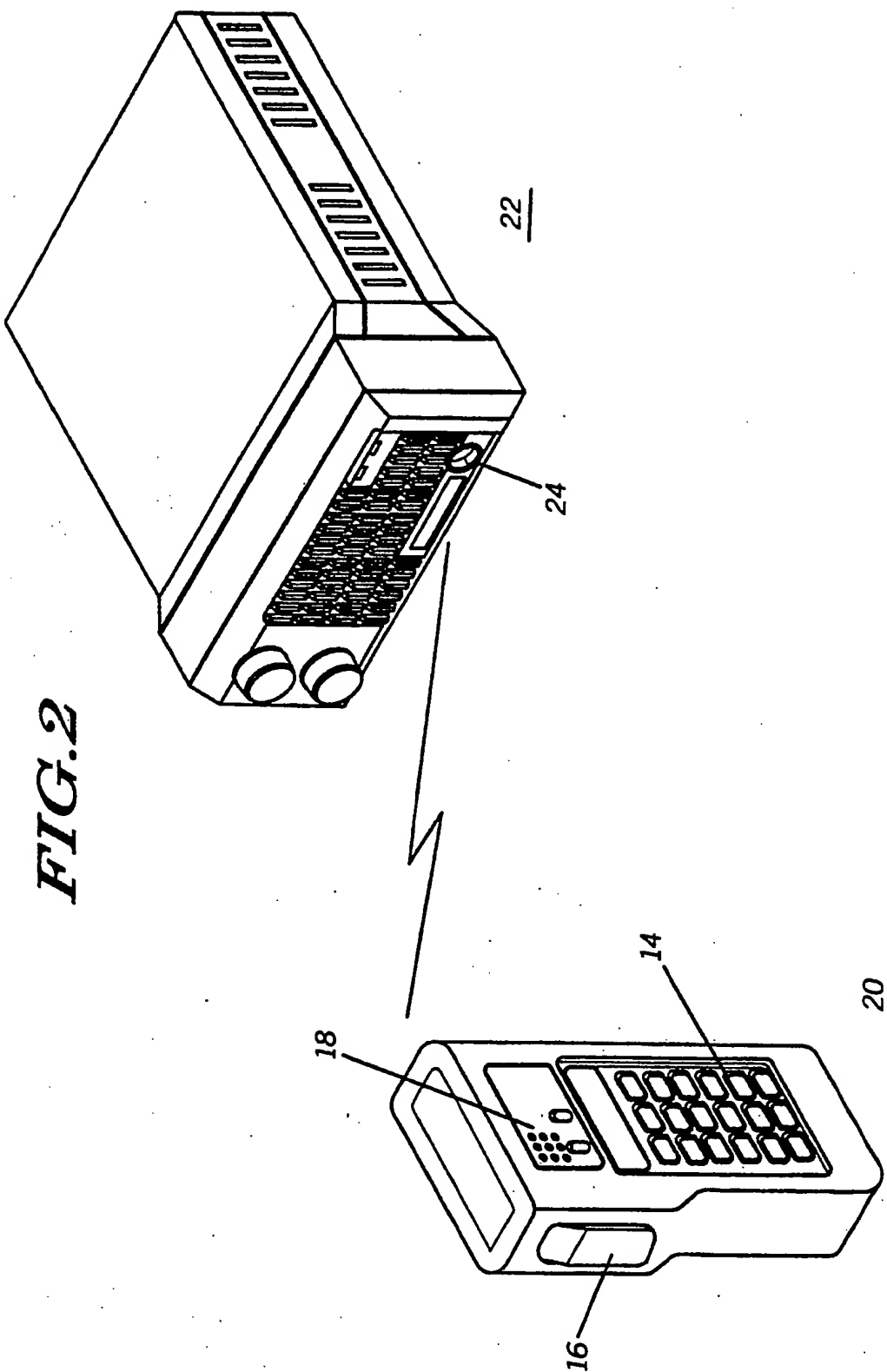
A communication device may be programmed to recognize voice commands via a portable programming apparatus. An identification code is employed to access particular voice recognition information (codebook) from a repository of voice recognition codebooks contained within the portable programming device. The programming device responds by transmitting the identified codebook to at least one communication device, which stores the codebook therein. Thereafter, the communication device may respond to the voice commands of that individual.

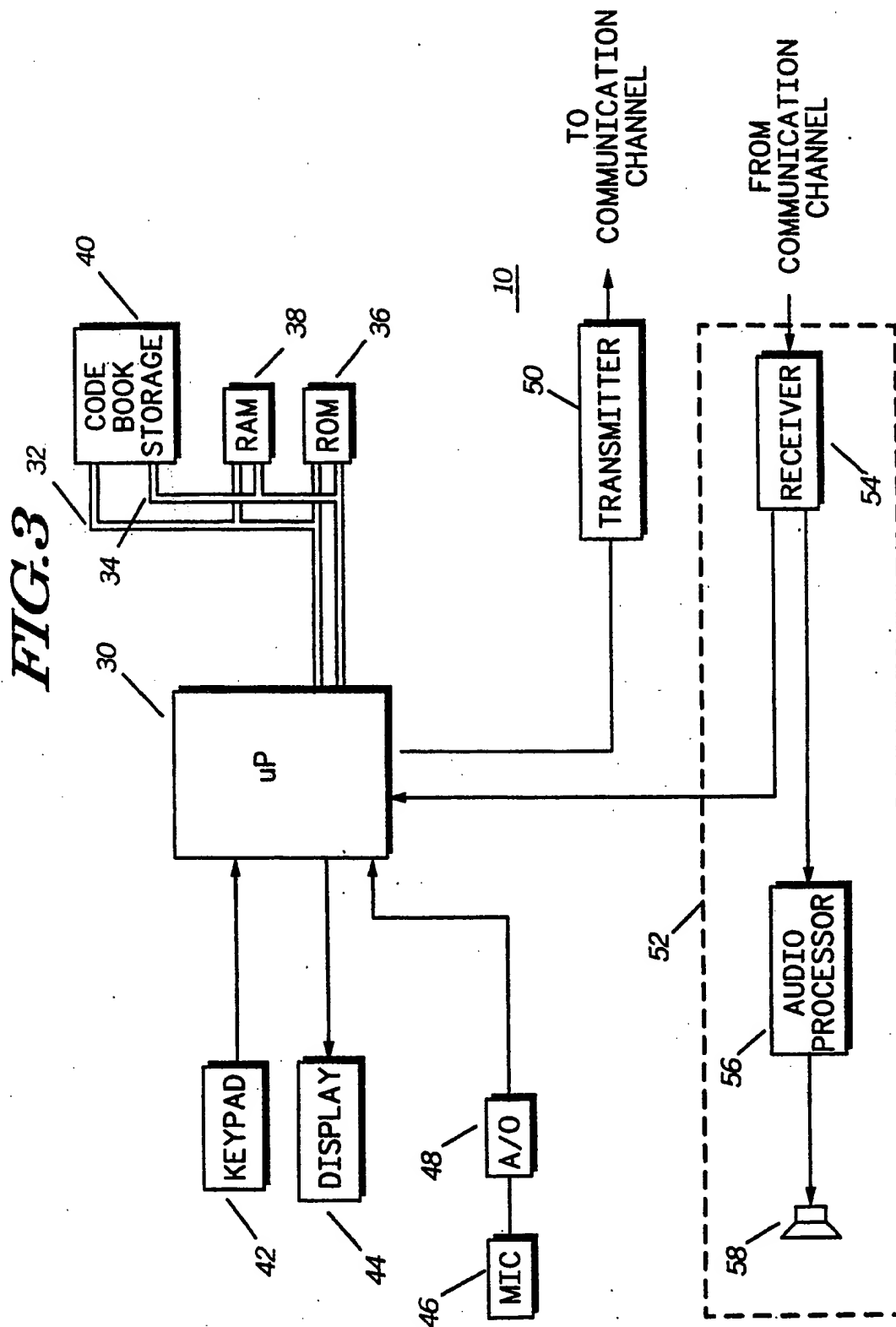
13 Claims, 4 Drawing Sheets



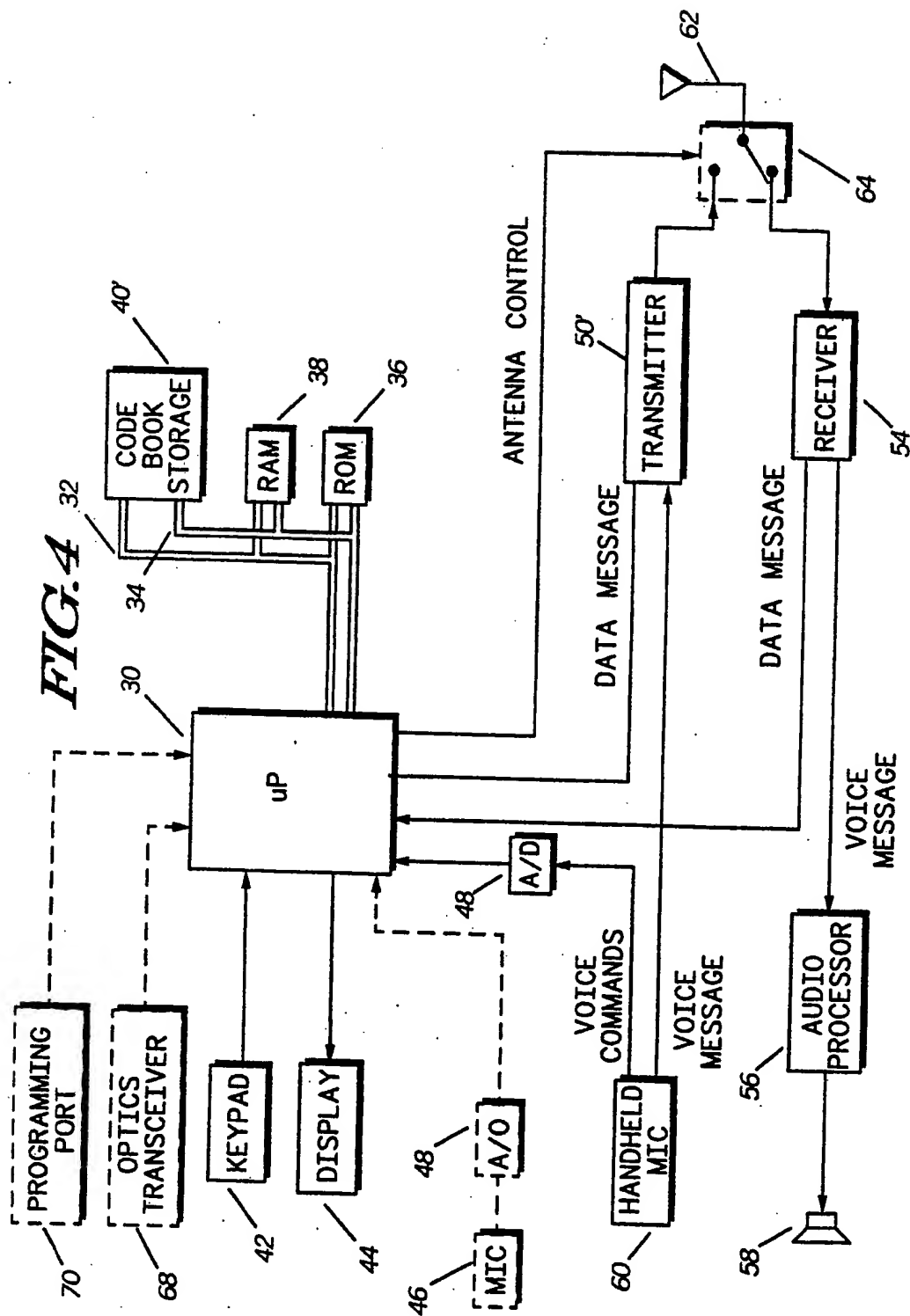
*FIG. 1*











## METHODS AND APPARATUS FOR PROGRAMMING DEVICES TO RECOGNIZE VOICE COMMANDS

This is a continuation of application of application Ser. No. 07/213,803 filed June 30, 1988 and now abandoned.

### TECHNICAL FIELD

This invention relates generally to voice recognition, and more particularly to speaker dependent voice recognition applied to information communication systems, and is more specifically directed toward a method for programming communication devices to recognize and respond to voice commands.

### BACKGROUND ART

Voice recognition technology has been recognized as an advantageous feature for many product applications. Such technology may be employed to render a product partially or entirely controllable by voice commands in situations where hands-on control is impossible or impracticable. Presently, however, voice recognition technology has not found wide use due to the complexity of its implementation, and requirements for a large amount of electronic storage (memory).

Speaker dependent voice recognition devices are designed to respond to a particular individual. Stored within such devices are speaker specific parameters, such as, for example, variations in the vocal tract response, pitch period, short-term speech power, and amplitude of the short-term speech spectra. In order for a speaker dependent device to respond to more than one person, the voice recognition information (commonly referred to as a "codebook") for each person must be stored within the device. However, mass codebook storage in each subscriber unit (radio) may prove impractical due to space or cost considerations. An alternative may be to use speaker independent technology, however, speaker independent devices are typically more complex and costly.

When applied to information communication devices, voice recognition technology raises several concerns. One major concern comprises the recognition that communication devices are typically used by more than one individual. For example, police vehicles are generally in service for three eight-hour shifts, during which at least three officers use the vehicle. Moreover, the officers using the vehicle (radio) may be anyone on the entire police force. Therefore, each radio must contain a codebook for each officer on the force. This would significantly increase the cost of the radios. Additionally, codebook maintenance costs would be significant since the radios must be updated with each change in personnel. Another concern is the increase in radio size. Contemporary state-of-the-art communication devices are designed so as to minimize their physical size. The addition of several memory devices, or a memory printed circuit board, may increase the size of the device beyond that desired by the consuming public. This is a particular concern in the personal pager and handheld radio products.

One solution may be to store the codebooks of only a few individuals thereby reducing the amount of required memory. However, this approach is inflexible to changing circumstances such as variations in personnel working hours or in the event that the radio itself

should fail. Another approach may be to have each radio contain only enough memory for a single codebook, which must be retrained for each person. Speaker dependent voice recognition devices must be "trained" to respond to each individual. Training is accomplished by having an individual repeat control words several times until the device has been "trained" to recognize that word as spoken by that individual. However, training is a time consuming process and may be very inefficient in certain markets, such as police and fire protection, where rapid activity is ordinarily required. Accordingly, a need exists in the art to permit information communication devices to be programmed to respond to the voice commands of several individuals in an efficient and organized manner.

### SUMMARY OF THE INVENTION

Briefly, according to the invention, a communication device may be programmed to recognize voice commands via a portable programming apparatus. An identification code is employed to access particular voice recognition information (codebook) from a repository containing one or more voice recognition codebooks within the portable programming device. The programming device responds by transmitting the identified codebook to at least one communication device, which stores the codebook therein. Thereafter, the communication device may respond to the voice commands of that individual. In this way, the communication device may be rapidly reprogrammed to accommodate changing operators.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustration of a programming device in accordance with the present invention, and a vehicle having a mobile subscriber unit installed there;

FIG. 2 is an illustration of an alternate programming device in accordance with the present invention, and a mobile subscriber unit;

FIG. 3 is a block diagram of the programming device of FIG. 1 or FIG. 2;

FIG. 4 is a block diagram of a subscriber unit according to the present invention.

### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to FIG. 1, there is shown a radio frequency programming device (10) communicating with a vehicle (12) having a mobile subscriber unit installed therein. Preferably, the programming device (10) operates as a repository of all of the codebooks for individuals that may operate the subscriber unit. Alternately, the total collection (or library) of codebooks may be apportioned between two or more programming devices.

The subscriber units may be mobile units, portable units, or control stations. Generally, a portable subscriber unit is designed to be carried on or about the person, a mobile subscriber unit is designed to be mounted into vehicles, and control stations are permanent or semi-permanent installations installed in buildings or other fixed locations. As used herein, the term subscribers collectively refers to portable units, mobile units or control stations.

As mentioned above, preferably all required codebooks for all personnel using a communication system are centrally contained in the programming device (10). The programming device thus becomes a central reposi-

tory (library) of the several codebooks. Preferably, a separate facility may be used to provide "training" of the subscriber units. For example, all codebooks for an entire police force may be created by training a subscriber unit (or its simulated equivalent) at the police station, after which the newly created codebooks may be transferred to the programming device via any convenient means. In this way, the codebook library may be maintained. Alternately, the programming device may allow for creation of codebooks by having subscriber operators train the programming device itself.

Each of the subscriber units contain enough codebook memory to store the codebook for at least one individual. Thus, before an individual may use the subscriber unit, his or her codebook must be transferred from the programming device (10) to the subscriber unit. Preferably, codebook transfer is accomplished by entering a codebook identification code on a keypad (14) and depressing a transfer activation button (or switch) (16). The present invention also contemplates several alternatives to effect codebook transfer. One alternate comprises providing each operator with an identification card (or module) that may be inserted into the programming device, which causes an automatic transfer of the appropriate codebook from the programming device (10) to the subscriber unit. In another embodiment, the programming device may itself be voice controlled (speaker dependent) to transfer an identified codebook. In this way, codebook transfer could be controlled since the programming device would only respond to a limited number of speakers. In a further embodiment, the programming device may employ a limited version of speaker independent voice recognition technology, which may be used to effect codebook transfer.

In several circumstances, the operator of the mobile subscriber unit also carries an associated portable subscriber unit, which may be used to maintain communication when the operator is out of the vehicle. Accordingly, the present invention contemplates that the programming device (10) may simultaneously transfer a codebook to a mobile subscriber unit and its associated portable unit.

Once the codebook has been stored in a subscriber unit, the operator may partially (or entirely) control the operation of the subscriber unit by voice commands. Alternately, voice commands may be used in conjunction with manually entered commands (or vice versa) to execute a desired function. Whenever another individual desires to use that subscriber unit (for example, at a change in a working shift), the codebook for the new operator may be rapidly transferred as described above. Optionally, the memory in the subscriber may be expanded (within size and cost constraints) to retain a limited number of the last used codebooks in a first-in-last-out manner. For example, the codebook of the current user and the prior two operators may be retained in the subscriber unit. In this way, if the same three individuals operating the subscriber during the three operating shifts were ordinarily repeated day to day, no reprogramming of the subscriber unit would be required.

Referring now to FIG. 2, there is shown a programming device (20) communicating via modulated light waves (optics) with a subscriber unit (22). For example, infrared scattering light may be used to transfer the codebook from the programming device to the subscriber unit. As discussed in conjunction with FIG. 1, a

codebook transfer is preferably accomplished by entering a codebook identification code on a keypad (14) and depressing a transfer activation button (or switch) (16). Alternately, identification cards (or modules) may be used to cause an automatic transfer of the appropriate codebook from the programming device (10) to the subscriber unit. Also, the programming device may itself be voice controlled (using speaker dependent or independent technology) to transfer an identified codebook. Lastly, as an alternative to either radio frequency or light wave communication, codebook transfer may be effected via an interface cable (either conductive wire or fiber optic link) between a programming port (24) on the subscriber unit (22), and a programming port (24') on the programming device (10 or 20).

Referring now to FIG. 3, there is shown a block diagram of the programming unit (10 or 20). The programming unit operates under the control of a microprocessor (30), which communicates via an address bus (32) and a data bus (34) with read-only memory (ROM) (36) and random access memory (RAM) (38). The codebook for each individual resides in mass codebook storage (40), which preferably comprises electronically erasable programmable read-only memory (EEPROM). Alternately, battery backed-up RAM may be used.

The operator may enter manual commands via the keyboard (42), and receive status or information updates by the display (44). Preferably, in a voice controlled programmer embodiment, voice commands are entered via the microphone (46), which are digitized (48) and processed by the microprocessor (30). Codebook transfer is accomplished via a transmitter (50), which is of a type in accord with the particular communication media employed. That is, an optics transmitter for fiber optic cable or infrared scattered transmission, a radio frequency transmitter for RF communication, or merely a modulator amplifier for wireline transmission. Optionally, the programming device (10) may include a receiver section (52) comprising a receiver (54), which may forward data messages, such as acknowledge messages, to the microprocessor (30), while routing analog messages (such as a programming complete or error signal) to any suitable audio processing stages (56), which may provide an alert tone to the operator via the speaker (58).

Referring now to FIG. 4, there is shown a block diagram of a subscriber unit (22) according to the invention. The subscriber unit also operates under the control of a microprocessor (30), which communicates via an address bus (32) and a data bus (34) with read-only memory (ROM) (36) and random access memory (RAM) (38). The codebook for at least one individual resides in the codebook storage (40'), which preferably comprises electronically erasable programmable read-only memory (EEPROM). Alternately, battery backed-up RAM may be used.

The operator may enter manual commands via the keyboard (42), and receive status or information updates by the display (44). Preferably, voice commands are entered via the handheld microphone (60), which are digitized (48) and processed by the microprocessor (30). Optionally, a condenser microphone (or equivalent) (46) may be mounted on the subscriber unit, to receive voice commands without the necessity of picking up the handheld microphone (60). Voice messages are transmitted via the handheld microphone (60) and a radio frequency transmitter (50'), which may also trans-

mit data messages from the microprocessor (30). The transmitter (50') is selectively coupled to the antenna (62) via the antenna switch (64), which is controlled via the antenna control line (66) from the microprocessor (30). The subscriber unit (14) may also receive data or voice messages via a radio frequency receiver (54'), which forwards data messages to the microprocessor (30), while routing voice messages to any suitable audio processing stages (56), which may provide the voice messages or signalling tones to the operator via the speaker (58).

The subscriber unit (22) may accept a codebook for storage in a variety of ways. In a radio frequency programmer embodiment, a subscriber unit (22) may receive a codebook transmitted from a programming device (10) via the antenna (62), which is coupled (64) to a receiver (54'). The receiver (54') routes the received codebook information to the microprocessor (30), which may store the codebook in the codebook storage (40'). Optionally, an acknowledge message may be transmitted (50') to the programming device (10) to confirm receipt of the codebook. In an optic programmer embodiment, the subscriber unit (22) is equipped with an optical receiver (or transceiver) (68) to enable the subscriber unit to receive a codebook transmitted by a programmer (20) via, such as, infrared scattering. Lastly, a subscriber may be provided a programming port (70), which may accommodate a wireline or fiber optic cable to enable the subscriber to receive a codebook.

According to the invention, a significant level of voice control, may be accomplished by a limited word set. While total voice control may require several additional words, the present invention contemplates that the subscriber unit may be at least partially controlled by the word set as represented in Table 1 below.

TABLE 1

EMERGENCY  
LIGHTS  
SIREN  
ON  
OFF  
MONITOR  
CANCEL  
STATUS  
TRANSMIT  
RECEIVE  
DISPLAY  
SCAN  
DIAL  
CALL  
CHANNEL  
ACKNOWLEDGE  
MESSAGE  
NUMBER  
ZERO  
ONE  
TWO  
THREE  
FOUR  
FIVE  
SIX  
SEVEN  
EIGHT  
NINE

In summary, the present invention provides that a communication device may be programmed to recognize voice commands via the portable programming apparatus described above. To effect codebook transfer, the programming device receives an identification code, which is used to access particular voice recognition information from a repository of codebooks contained within the portable programming device. The identified codebook is transferred to at least one communication device by modulated radio waves, modulated light waves, or other suitable modulated electronic signals. Upon receipt and storage of the codebook, the communication device may respond to the voice commands of that individual. In this way, the communication device may be rapidly reprogrammed to accommodate changing operators.

What is claimed is:

1. In a communication system having at least one communication unit being at least partially controlled by voice commands, a method for programming said at least one communication unit to recognize said voice commands, comprising the steps of:

at a programming device having a repository of voice recognition information for at least two individuals stored therein:

(a) receiving a code identifying data representing at least voice recognition information for at least one individual;

(b) programming said at least one communication unit to recognize voice commands by transmitting at least said data representing at least voice recognition information via modulated radio frequency or optical signal to said at least one communication unit;

at said at least one subscriber unit:

(a) receiving said data representing at least voice recognition information from said at least one programming device.

2. The method of claim 1, which further comprises the step of;

(a1) coupling an interface means between said programming device and said communication unit prior to said programming step so as to be able to transmit said data representing at least voice recognition information.

3. The method of claim 1, wherein said programming device receiving step comprises: receiving a code entered on a keypad.

4. The method of claim 1, wherein said programming device receiving step comprises:

(a) receiving a voice signal;

(b) processing said voice signal to identify said data representing at least voice recognition information;

(c) programming said at least one communication unit to recognize voice commands to transmitting at least said data representing at least voice recognition information via modulated radio frequency or optical signal to said at least one communication unit.

5. The method of claim 1, which includes the communication unit steps of:

(b) processing, in the absence of manually entered commands, voice commands in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said voice commands;

7

(c) processing, when said manually entered commands are present, said manually entered commands in cooperation with said voice commands processed in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said manually entered commands and said voice commands.

6. The method of claim 1, which includes the communication unit step of: (b) processing voice commands at said subscriber unit in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said voice commands.

7. The method of claim 1, which includes the communication unit step of: storing at least a portion of said data representing at least voice recognition information.

8. In a communication system having at least one communication unit being at least partially controlled by voice commands, a method for programming said at least one communication unit to recognize said voice commands, comprising the steps of:

at a programming device having a repository of voice recognition information for a plurality of individuals stored therein:

(a) receiving a code identifying data representing at least voice recognition information for at least one individual;

(b) programming said at least one communication unit to recognize voice commands by transmitting at least said data representing at least voice recognition information via modulated radio frequency or optical signal to said at least one communication unit;

at said at least one communication unit;

(a) receiving said data representing at least voice recognition information from said at least one programming device;

(b) storing at least a portion of said data representing at least voice recognition information;

(c) processing, in the absence of manually entered commands, voice commands in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said voice commands;

(d) processing, when said manually entered commands are present, said manually entered commands in cooperation with said voice commands processed in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said manually entered commands and said voice commands.

9. In a communication system having at least one communication unit being at least partially controlled by voice commands, a method for programming said at least one communication unit to recognize said voice commands, comprising the steps of:

at a programming device having a repository of voice recognition information for at least two individuals stored therein:

(a) receiving a code identifying data representing at least voice recognition information for at least one individual;

(b) programming said at least one communication unit to recognize voice commands by transmitting at least said data representing at least voice recog-

8

nition information via modulated radio frequency or optical signal to said at least one communication unit;

at said at least one communication unit:

(a) receiving said data representing at least voice recognition information from said at least one programming device;

(b) storing at least a portion of said data representing at least voice recognition information;

(c) processing voice commands at said communication unit in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said voice commands.

10. In a communication system having at least one communication unit being at least partially controlled by voice commands, a method for programming said at least one communication unit to recognize said voice commands, comprising the steps of:

at a programming device having a repository of voice recognition information for at least two individuals stored therein:

(a) receiving a voice signal representing at least a code identifying data representing at least voice recognition information for at least one individual;

(b) transmitting at least said data representing at least voice recognition information via modulated radio frequency or optical signals to said at least one communication unit;

at said at least one communication unit:

(a) receiving said data representing at least voice recognition information from said at least one programming device;

(b) storing at least a portion of said data representing at least voice recognition information;

(c) processing voice commands at said communication unit in accordance with said data representing at least voice recognition information to at least partially control operation of said communication unit in response to said voice commands.

11. In a communication system having at least one communication unit being at least partially controlled by voice commands, a programming device comprising: means for receiving a code identifying data representing at least voice recognition information for at least one individual stored in a repository of voice recognition information for at least two individuals; and

programming means for programming said at least one communication unit to recognize voice commands, said programming means including transmitter means for transmitting at least said data representing at least voice recognition information via modulated radio frequency or optical signals to said at least one communication unit.

12. In a communication system having at least one communication unit being at least partially controlled by voice commands, a programming device comprising: means for receiving a voice signal representing at least a code identifying data representing at least voice recognition information for at least one individual stored in a repository of voice recognition information for a plurality of individuals; and programming means for programming said at least one communication unit to recognize voice commands, said programming means including transmitter means for transmitting at least said data representing at least voice recognition information

9

via modulated radio frequency or optical signals to said at least one communication unit.

13. A programming system for programming at least one communication unit to recognize voice commands, 5 comprising:

a programming device, comprising:

means for receiving a code identifying data representing at least voice recognition information for at 10 least one individual stored in a repository of voice

10

recognition information for at least two individuals;

means for transmitting at least said representing at least voice recognition information via modulated radio frequency or optical signals to said at least one communication unit;

said at least one communication unit, comprising: means for receiving said data representing at least voice recognition information from said at least one programming device.

\* \* \* \* \*

15

20

25

30

35

40

45

50

55

60

65



US006580972B1

(12) **United States Patent**  
**Strohbeck**

(10) Patent No.: **US 6,580,972 B1**  
 (45) Date of Patent: **Jun. 17, 2003**

(54) **DEVICE AND METHOD FOR  
 REPRODUCING INFORMATION IN A  
 MOTOR VEHICLE**

(75) Inventor: **Walter Strohbeck, Narre Wawen (AU)**

(73) Assignee: **Robert Bosch GmbH, Stuttgart (DE)**

(\*) Notice: Subject to any disclaimer, the term of this  
 patent is extended or adjusted under 35  
 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/936,846**

(22) PCT Filed: **Mar. 20, 2000**

(86) PCT No.: **PCT/DE00/00832**

§ 371 (c)(1),  
 (2), (4) Date: **Jan. 7, 2002**

(87) PCT Pub. No.: **WO00/57009**

PCT Pub. Date: **Sep. 28, 2000**

(30) **Foreign Application Priority Data**

Mar. 22, 1999 (DE) ..... 199 12 748

(51) Int. Cl.<sup>7</sup> ..... **G06F 7/00; B60R 25/00**

(52) U.S. Cl. .... **701/1; 701/32; 701/36;  
 307/10.3; 307/10.5**

(58) Field of Search ..... **701/1, 2, 29, 33,  
 701/36, 32; 307/9.1, 10.1, 10.2, 10.3, 10.5,  
 10.6**

(56) **References Cited**

#### U.S. PATENT DOCUMENTS

5,513,107 A 4/1996 Gormley ..... 701/48  
 5,552,641 A 9/1996 Schneider et al. .... 307/10.5

#### FOREIGN PATENT DOCUMENTS

DE	196 480 42	5/1998
DE	197 28 226	1/1999
EP	0 592 166	4/1994
EP	0 762 339	3/1997
EP	0 924 123	6/1999
FR	2 752 004	2/1998

*Primary Examiner*—William A Cuchlinski, Jr.

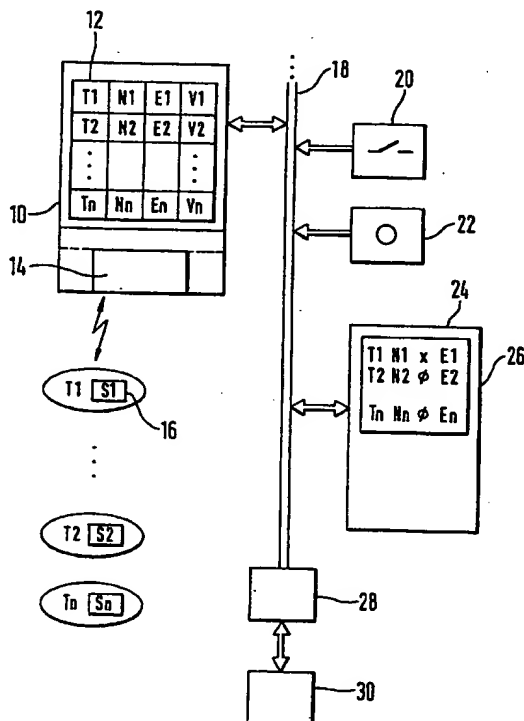
*Assistant Examiner*—Edward Pipala

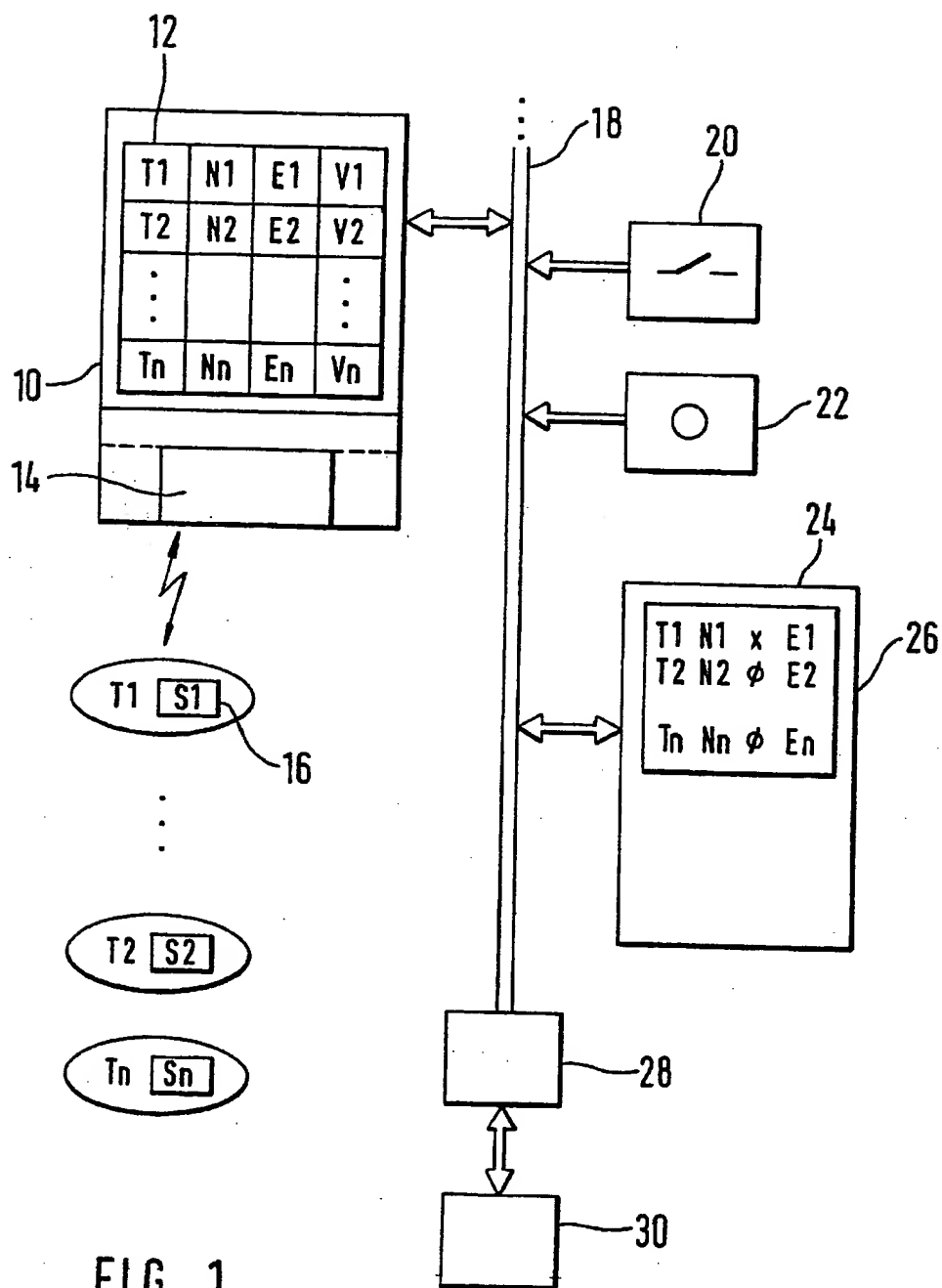
(74) *Attorney, Agent, or Firm*—Kenyon & Kenyon

(57) **ABSTRACT**

A device and a method for reproducing information in a motor vehicle include, as part of a keyless access system and/or drive authorization system, a portable transponder for sending a code via a transceiver to a control device arranged in the motor vehicle. Access authorization and/or drive authorization are granted if the control device receives a valid code. A display is arranged in the vehicle. The display displays specific data based on an output signal from the control device.

**12 Claims, 2 Drawing Sheets**







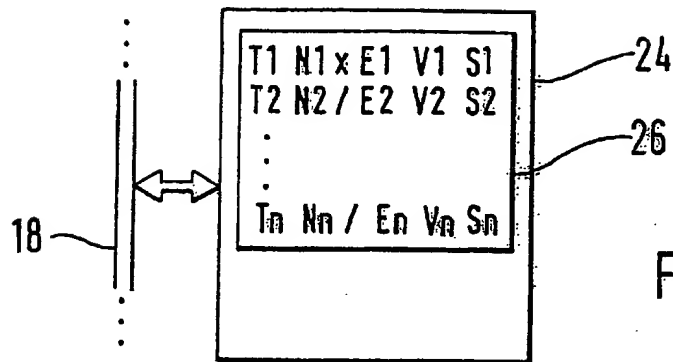


FIG. 2

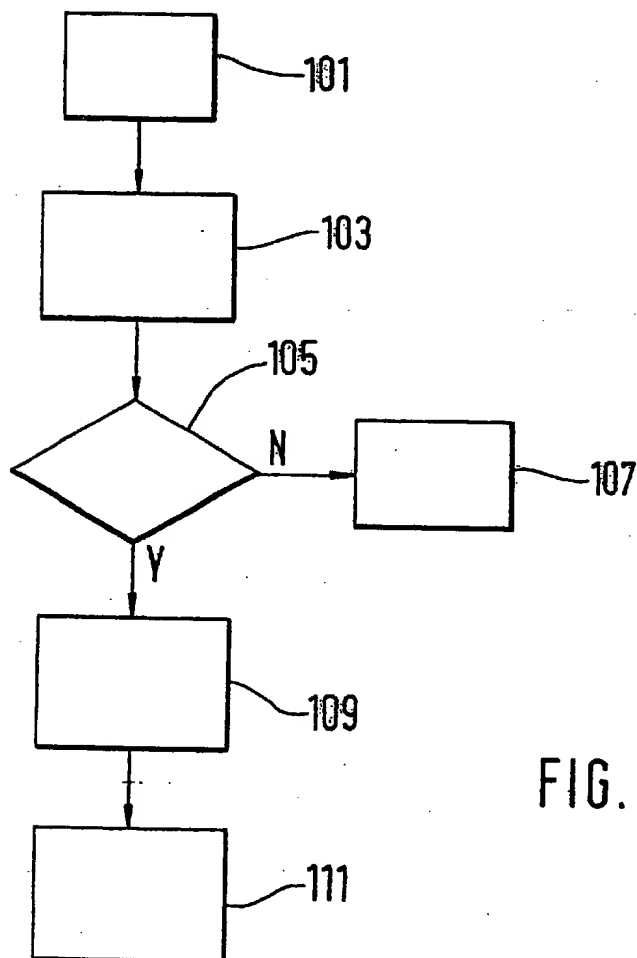


FIG. 3

1

## DEVICE AND METHOD FOR REPRODUCING INFORMATION IN A MOTOR VEHICLE

### FIELD OF THE INVENTION

The present invention relates to a device and a method for reproducing information in a motor vehicle.

### BACKGROUND INFORMATION

In German Published Patent Application No. 196 480 42 is discussed a motor vehicle having a key for identifying an authorized user. Data such as the customer's address, the vehicle ID number, or the odometer reading are stored in the key. At a workshop the key is placed in a read device, which is connected to a computer and on whose screen a dialog is carried out in order to read out the key data. However, the data can only be displayed if a password is entered manually.

This device may only be suitable for reading out pertinent data if it is used in conjunction with an external device.

### SUMMARY OF THE INVENTION

An object of an exemplary embodiment and/or exemplary method of the present invention is to provide a display device having additional functions, for normal use of the vehicle.

An exemplary device according to the present invention for reproducing information in a motor vehicle includes one (or a plurality) of portable transponders as part of a keyless access system and/or drive authorization system, which sends a code to a control device inside the vehicle. Access authorization and/or drive authorization is granted if the control device receives a valid code. It includes a display, which is arranged inside the vehicle. The display displays specific data based on an output signal from the control device.

The display can only be activated if a valid code transmitted by the transponder is received. The pertinent data are only made available to a user who has thus demonstrated that he is authorized. Other persons who are not in possession of a valid transponder cannot gain access to these data. Based on the code received, the display can be updated automatically, further operating signals from the user not being necessary to accomplish this. Therefore, the code signal from a transponder is suitable for this initiation procedure for the display, as the code signal transmission procedure is already carried out before initiation of the start procedure for the vehicle. Thus, the user can be supplied with pertinent information about the vehicle's operating condition in advance before he operates the ignition. The code signal of a transponder is triggered automatically upon operation of the outside door handle, the ignition/start switch, and the remote control button of the transponder (if present).

According to another exemplary embodiment, the data is also displayed if a further operating element, a door contact, has been operated. The combination of the transponder query and an output signal from an operating element provides security against unauthorized access to the data, and the display is not activated until the instant when operation of an operating element indicates that the user is inside the vehicle.

According to another exemplary embodiment, data which depend directly on the code received by the control device is transmitted to the display. To accomplish this, the control

2

device sends out a search signal which addresses all transponders assigned to the vehicle. The transponders that are located within the control device's transmission range send back a corresponding answer signal. Based on the incoming signals, the control device can determine which transponders are present. This information is forwarded to the display. Thus, the user is informed of which transponders are located inside the vehicle. In particular, this information reminds the driver before he leaves the vehicle that he should take the transponders that are in the vehicle with him so as to reduce the risk of unauthorized starting of the vehicle.

The display duration may be limited to a predefined time. This should at least better ensure that no operation intervention to support the functionality of the exemplary method should be necessary. According to another exemplary embodiment, the current display duration is extended by a further full basic duration if a further trigger event occurs before the predefined display time has elapsed. In addition to straightforward timer control, the display duration can also be coupled to the occurrence of a further event. This event may be the starting and/or stopping of the engine or the locking of the vehicle.

The exemplary method according to the present invention for reproducing information in a motor vehicle may use a portable transponder as part of a keyless access system and/or drive authorization system which transmits a code via a transceiver to a control device arranged inside the vehicle, access authorization and/or drive authorization being granted if the control device receives a valid code. A display is arranged inside the vehicle, the display displaying specific data based on an output signal from the control device. The exemplary method involves the following steps:

Transceiver sends out a search signal which causes the transponder to send back a code;

The control device evaluates the code received via the transceiver; and

The display is activated.

The data exchange carried out in connection with the authorization query provides information as to which transponders are located within the transceiver's coverage range. This information is forwarded to the display in the next step, and is available to the user immediately. According to another exemplary embodiment, the display is also triggered even if no code or an unauthorized code is received during a time period that begins with the sending out of the search signal. The user can be made aware of this critical situation immediately, as the corresponding query procedure for transponder recognition has already been carried out.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a block diagram.

FIG. 2 shows a further display.

FIG. 3 shows a flow chart relating to the exemplary embodiment and/or exemplary method.

### DETAILED DESCRIPTION

Memory 12 and transceiver 14 are arranged in control device 10. Transceiver 14 exchanges data with first transponder T1 and if necessary with second transponder T2 and nth transponder Tn. For each of these transponders T1, T2, Tn, an accompanying name N1, N2, Nn of a transponder user, settings E1, E2, En, and confidential data V1, V2, Vn are stored in memory 12. In each of transponders T1, T2, Tn, special data S1, S2, Sn are stored in a memory. Control

3

device 10 communicates via bus system 18 with display unit 24, which includes display 26. A signal from door switch 20 and a signal from operating element 22 are conveyed to bus system 18. Diagnosis interface 28 via which, in conjunction with input/output unit 30, data can be read in or out, is provided on bus system 18. In normal operating mode, names N1, N2, Nn, binary information (x, 0) and settings E1, E2, En that are assigned to transponders T1, T2, Tn are displayed to the user via a display.

In a special operating mode, name N1, N2, Nn, the binary information, settings E1, E2, En, confidential data V1, V2, Vn and special data S1, S2, Sn that are assigned to the transponders T1, T2, Tn in question appear on the display; as an alternative, just parts of this information are displayed.

The flow chart shown in FIG. 3 is now used for describing the exemplary method and/or how the exemplary device according to the present invention functions. A user who is in possession of first transponder T1 approaches the vehicle. In order to achieve access authorization, he operates the door handle (Step 101). The corresponding signal exchange is evaluated by control device 10. Transceiver 14 of control device 10 thereupon sends out a search signal. First transponder T1, which is within the range of transceiver 14, sends back an answer signal/code to control device 10. Based on the answer signal sent back, control device 10 determines which transponders T1, T2, Tn are located within the range of transceiver 14.

The evaluation as to which transponder T1, T2, Tn is present may be performed using, for example, a characteristic transmission time delay for the answer signal which distinguishes transponders T1, T2, Tn from each other. Each transponder T1, T2, Tn is assigned a corresponding time slot. If an answer signal is received within this characteristic time slot, control device 10 determines that transponder T1, T2, Tn that answers within this time slot is within range. Based on this evaluation procedure, the binary information is generated as to whether the transponder in question T1, T2, Tn is present (x) or not (0).

Triggering of the authorization query in Step 103 can also be carried out or performed in conjunction with opening or closing of the doors, or upon operation of an operating element in conjunction with a start or stop procedure of the vehicle. In this context, these transceivers 14 which cover the vehicle interior are triggered with a view to sending out a search signal. The incoming signals from transponders T1, T2, Tn may be used to determine which transponders T1, T2, Tn are located inside the vehicle. In Step 111, this information is made available to the display.

Provided a valid answer signal is received at transceiver 14, authorization query 103 is carried out next. To accomplish this, a signal is sent to first transponder T1, which has been recognized as being present, and is processed by first transponder T1. First transponder T1 sends the processed signal back as a code. At the same time, the identical procedure for determining the expected code is carried out in control device 10.

If the incoming code from first transponder T1 matches the expected code, the authorization procedure is deemed to have been carried out successfully (Step 105). If they do not match, the authorization procedure is terminated so that there is no result (Step 107). Based on the authorization query (Step 103), either authorization for access to the vehicle, or a drive authorization, which enables the control devices required for operation and thus allows the driver to start the engine, is granted. If the authorization query has been carried out successfully, control device 10 transmits a

4

command signal and the data to be displayed, such as transponder T1, T2, Tn, name N1, N2, Nn, transponder-dependent binary information, and settings E1, E2, En, to display unit 24 via bus system 18.

This data is merely an example. Any desired information may be displayed. Thus for each transponder T1, T2, Tn the name N1, N2, Nn of the transponder user in question is stored in memory 12 of control device 10. This is shown on the screen of display 26 in alphanumeric form. Settings E1, E2, En may constitute information as to whether the transponder T1, T2, Tn is blocked for an authorization query. Similarly, transponder-dependent user settings E1, E2, En could constitute a seat adjustment setting, a mirror adjustment setting or the like. Display unit 24 prepares the data made available by control device 10 and triggers display 26. This data is visible on display 26 for a predefined length of time.

According to another exemplary embodiment, the data is only displayed if the authorization query per Step 103 has successfully been carried out and also an additional event occurs. This additional event could be, for example, the closing of the doors, this being signaled via the signal status of door switch 20. Control device 10 then forwards a corresponding display command to display unit 24. Operation of operating element 22 may also constitute an event that triggers display 26. For example, the user would have to operate the ignition switch or the ignition lock in order for display 26 to be triggered. However, first an authorization query (Step 103) would have to have been successfully carried out. The data stored in memory 12 may also be read in and out via diagnosis interface 28 and the accompanying input/output unit 30. This may also be used, for example, when the device is started up for the first time.

In addition to the use of the display in normal mode as described above, in special mode protected data can be queried and overwritten. This protected data may be located in control device 10, in transponder T1, T2, Tn, or in both components. As this data is access-protected, the special-mode operation of display 26 has to be initiated via a suitable operating sequence. To accomplish this, one option is for the ignition to be switched on and off a plurality of times. This special operating sequence causes control device 10 to carry out a first authorization query with a first transponder T1, as described above in connection with Step 103.

According to the exemplary embodiment and/or exemplary method of the present invention, at least one further authorization query with a further transponder T2, Tn must be successfully carried out in order for the special mode data to be displayed. Provided the authorization query has been carried out successfully with a further transponder T2, Tn, control device 10 prepares the special mode data to be displayed. The queries described above may be carried out or performed in a single step. For read mode, two transponders T1, T2 may be enough; for write mode, e.g., entering a new owner, all valid transponders T1, T2, Tn must be available for querying. The number of valid transponders T1, T2, Tn can be determined from the contents of the memory, and allows the write mode to be enabled once the number of transponders T1, T2, Tn has been determined and the subsequent comparison has been carried out.

In addition to, or also independently of, the data already displayed in normal mode, in special mode confidential data V1, V2, Vn and/or special data S1, S2, Sn stored in transponders T1, T2, Tn may also be displayed (see FIG. 2). Control device 10 transmits a suitable command via trans-

5

ceiver 14 to the transponders T1, T2, Tn that are in range, so as to cause them to send back the special data S1, S2, Sn in question. Special data S1, S2, Sn and the data stored in memory 12 are forwarded to display unit 24 via bus system 18 with the help of an appropriate special display command.

Display 26 is now structured as shown in FIG. 2. Confidential data V1, V2, Vn and special data S1, S2, Sn may constitute information regarding the transponder owner, the address, service information regarding the vehicle, the vehicle's official ID, the vehicle registration certificate, the motor vehicle certificate, the chassis number, the engine number, or the insurance number. Thus, there is no need for an external read-out device. As described herein, it is easy for the workshop staff to access the data provided they are in possession of the necessary number of valid transponders T1, T2, Tn. If the vehicle's owner changes, data can be changed and the changes verified with the help of display 26 and input/output unit 30, provided all authorized transponders T1, T2, Tn are presented.

According to another exemplary embodiment, display 26 is also triggered if the authorization query carried out in Step 103 does not indicate a valid code or no code is received by transceiver 14 within a time period that begins when the search signal is sent out. Instead of immediate termination, Step 107 could also be used to trigger display unit 24 with a view to issuing a warning indicating "unauthorized transponder" or "no transponder." However, security-relevant information would not be displayed. In conjunction with a warning signal, display 26 may also be supported by visual or acoustic means (radio, or, for example, a piezoelectric signal generator).

Memory 12 may also be arranged in any other control device. In normal mode, data stored in transponders T1, T2, Tn may also be sent to display 26, the necessary transfer being carried out. Furthermore, transceiver 14 and control device 10 do not have to be structurally integrated. Instead, a plurality of transceivers 14 may be arranged at different points in the vehicle so as to ensure reliable detection of transponders T1, T2, Tn that are present. According to other exemplary embodiments, the signals from door switch 20 and/or operating element 22 are transmitted directly to control device 10. In addition to a visual display 26, the display unit 24 may be a display that merely indicates the transponders that are present via a back-lit display, or it may be an acoustic display. The door switches and tailgate switches may be connected directly to control device 10 to trigger the authorization query and/or display activation. The operating element 22 may be integrated into display unit 24. Furthermore, the authorization query described in connection with Steps 101 and 103 may be carried out in a single step and with one-time sending back of a transponder signal that is evaluated for authorization purposes.

What is claimed is:

1. A device for use as part of at least one of a keyless access system and a drive authorization system for reproducing information in a motor vehicle, the device comprising:

6

at least one portable transponder for transmitting a code via a transceiver to a control device arranged in the motor vehicle, at least one of access authorization and drive authorization being granted if the control device receives a valid code; and

a display arranged in the vehicle for displaying specific data based on an output signal from the control device.

2. The device of claim 1, wherein the specific data is displayed if the valid code is received by the control device.

3. The device of claim 1, wherein the specific data is displayed if at least one of an operating element and a door contact have been operated.

4. The device of claim 1, further comprising a second transponder, wherein the specific data is displayed if another valid code is received by the control device from the second transponder.

5. The device of claim 1, wherein the transceiver sends out a search signal for causing each portable transponder of the at least one portable transponder that is within a range to send back a respective code, so that each portable transponder within the range is recognizable.

6. The device of claim 1, wherein the specific data depends on whether the valid code is received.

7. The device of claim 1, wherein the specific data stored in at least one of the at least one portable transponder and the control device is displayed.

8. The device of claim 1, wherein the display includes at least one of an acoustic display and a visual display.

9. The device of claim 1, wherein the specific data stored in at least one of the control device and the at least one portable transponder is only accessible via an interface and an input/output unit if the valid code has been received.

10. A method for reproducing information in a motor vehicle, having, as part of at least one of a keyless access system and a drive authorization system, a portable transponder for transmitting a code via a transceiver to a control device arranged in the motor vehicle, at least one of an access authorization and a drive authorization being granted if the control device receives a valid code, and having a display arranged in the vehicle, the display being for displaying specific data based on an output signal from the control device, the method comprising:

sending out a search signal from the transceiver for causing the transponder to send back the code;

evaluating the code received via the transceiver using the control device; and

activating the display.

11. The method of claim 10, wherein the display is only activated if at least one received code is found valid.

12. The method of claim 10, wherein the display is activated if, after the search signal has been sent out, at least one of an invalid code and no code is received within a specific time period.

\* \* \* \* \*

# United States Patent [19]

Weber

[11] 3,784,839

[45] Jan. 8, 1974

[54] ANTI-THEFT APPARATUS INCLUDING  
TURNOVER MODE OF OPERATION

3,670,836 6/1972 Tonkowich et al. 307/10 AT  
3,653,457 4/1972 Lopez 180/114

[75] Inventor: John A. Weber, Franklin, Wis.

[73] Assignee: General Motors Corporation,  
Detroit, Mich.

[22] Filed: July 12, 1972

[21] Appl. No.: 271,141

Primary Examiner—J. R. Scott  
Assistant Examiner—M. Ginsburg  
Attorney—Eugene W. Christen et al.

[52] U.S. Cl. 307/10 AT, 180/114, 317/134  
[51] Int. Cl. B60r 25/00  
[58] Field of Search 307/10 AT; 317/134;  
340/63; 180/114

[56] References Cited

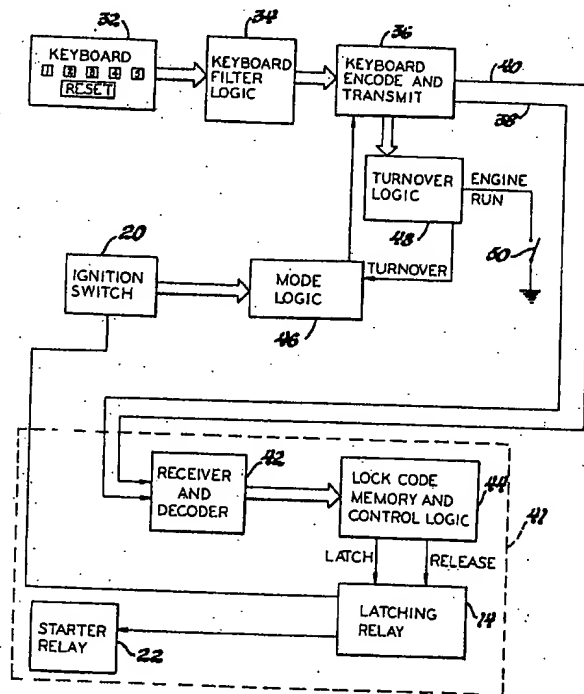
## UNITED STATES PATENTS

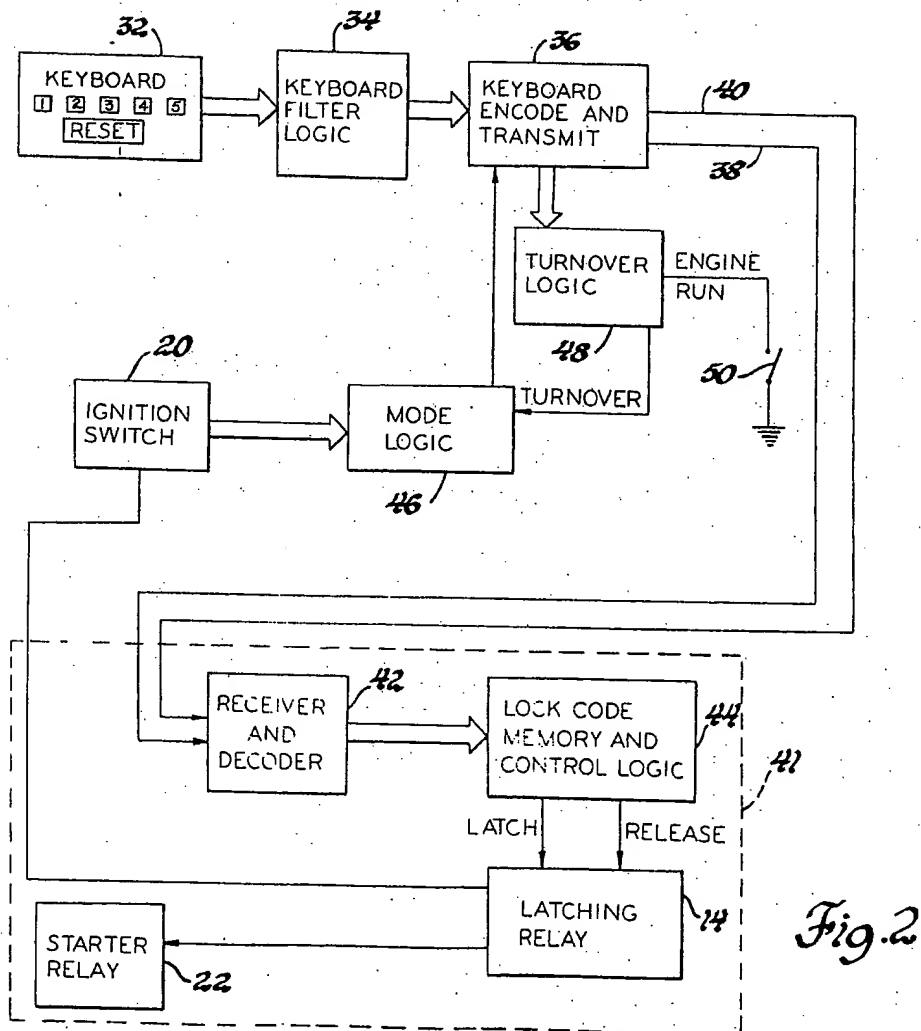
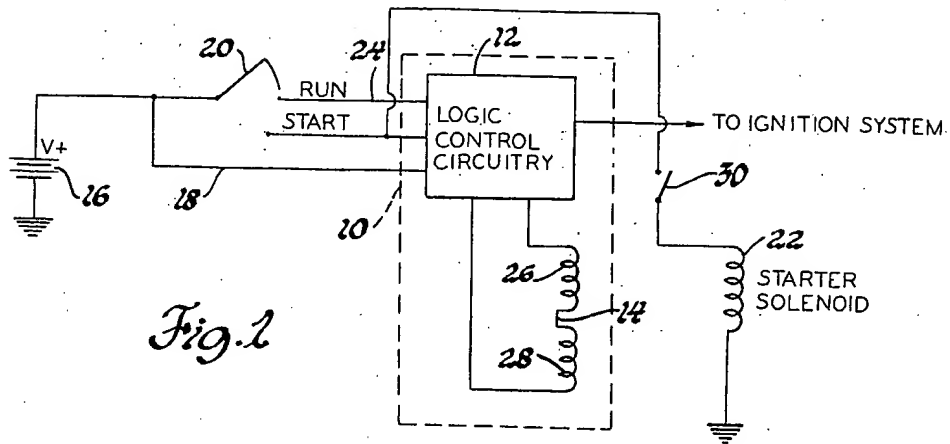
3,718,202 2/1973 Brock 307/10 AT

## [57] ABSTRACT

Starting of a motor vehicle is controlled from electronic combination lock circuitry which may be placed in a turnover mode of operation after the engine has been started to thereafter permit a predetermined number of engine starts without the entering of the lock combination.

2 Claims, 8 Drawing Figures





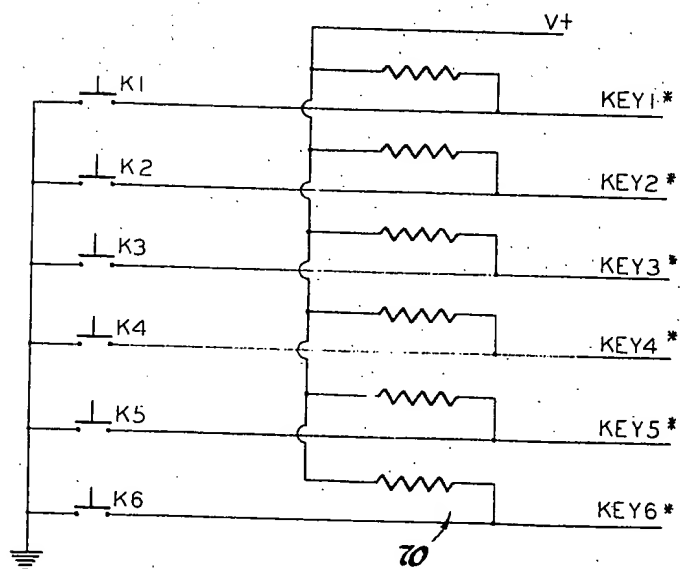
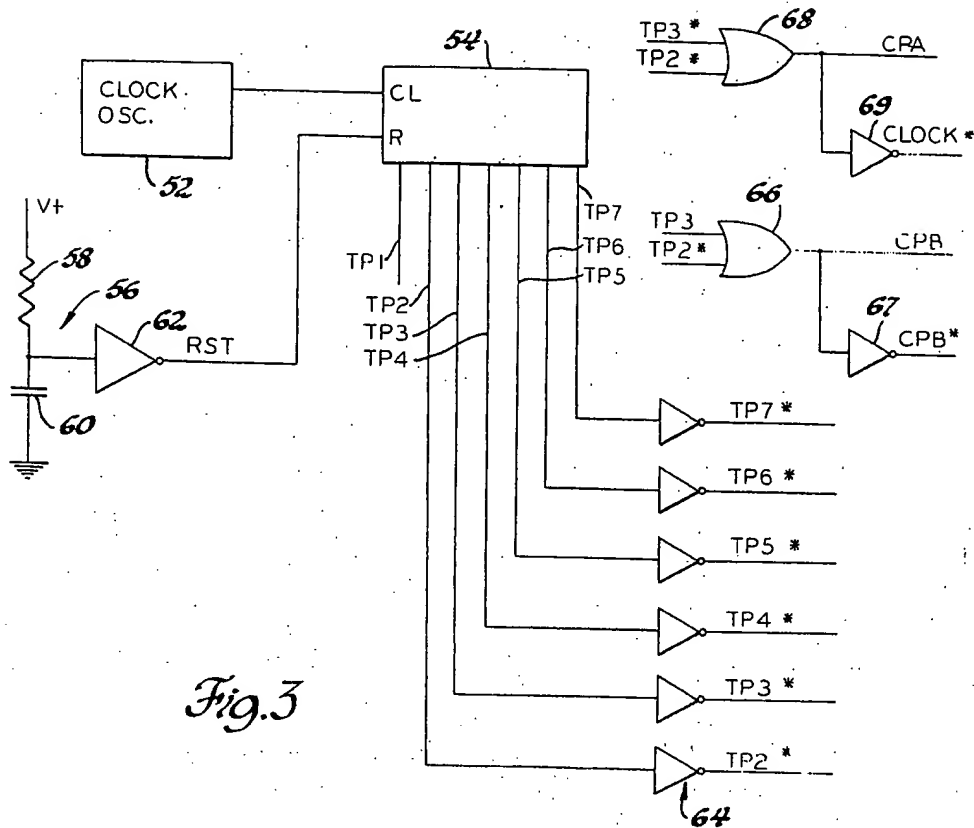


Fig. 4

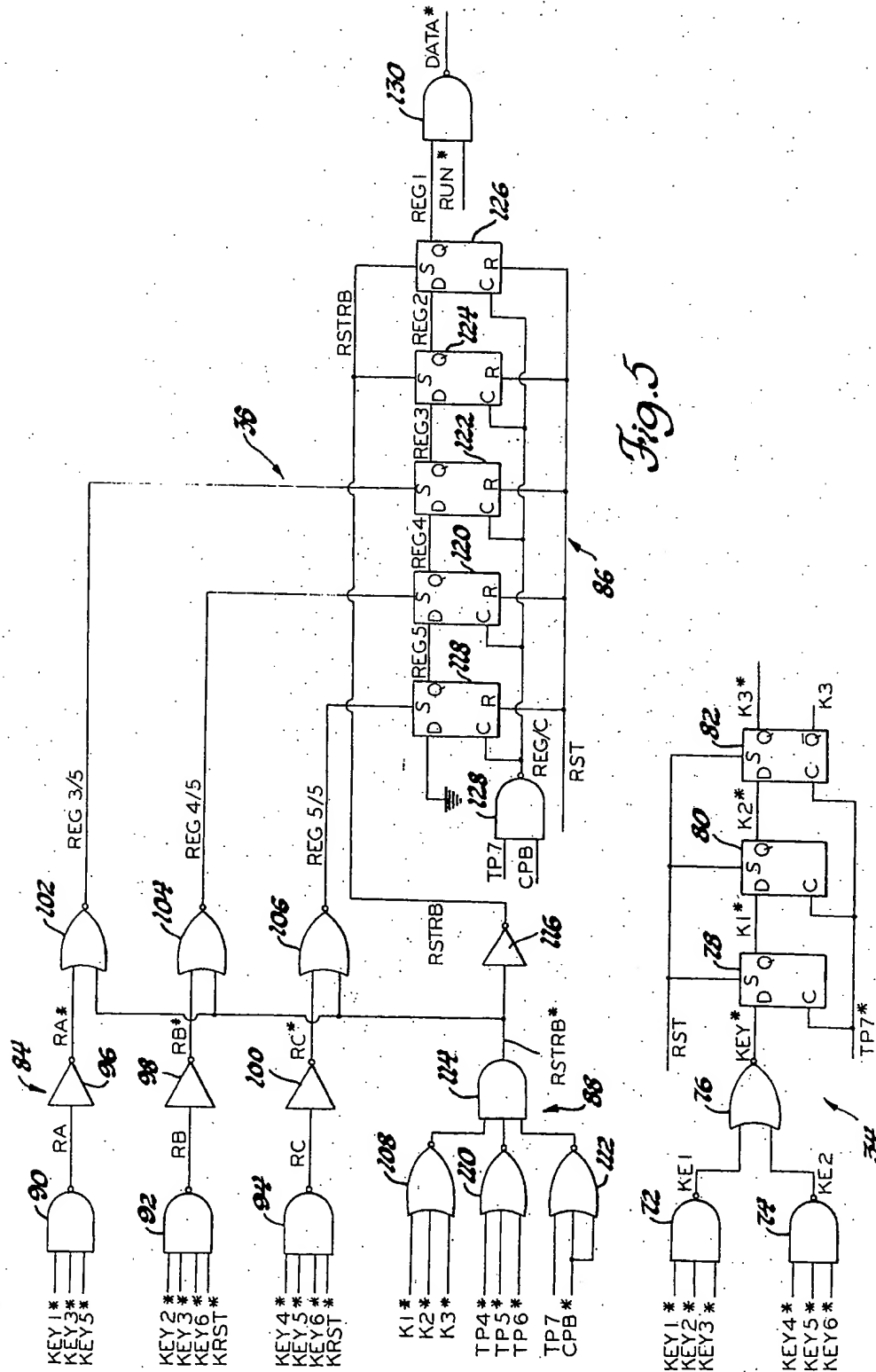


Fig. 5



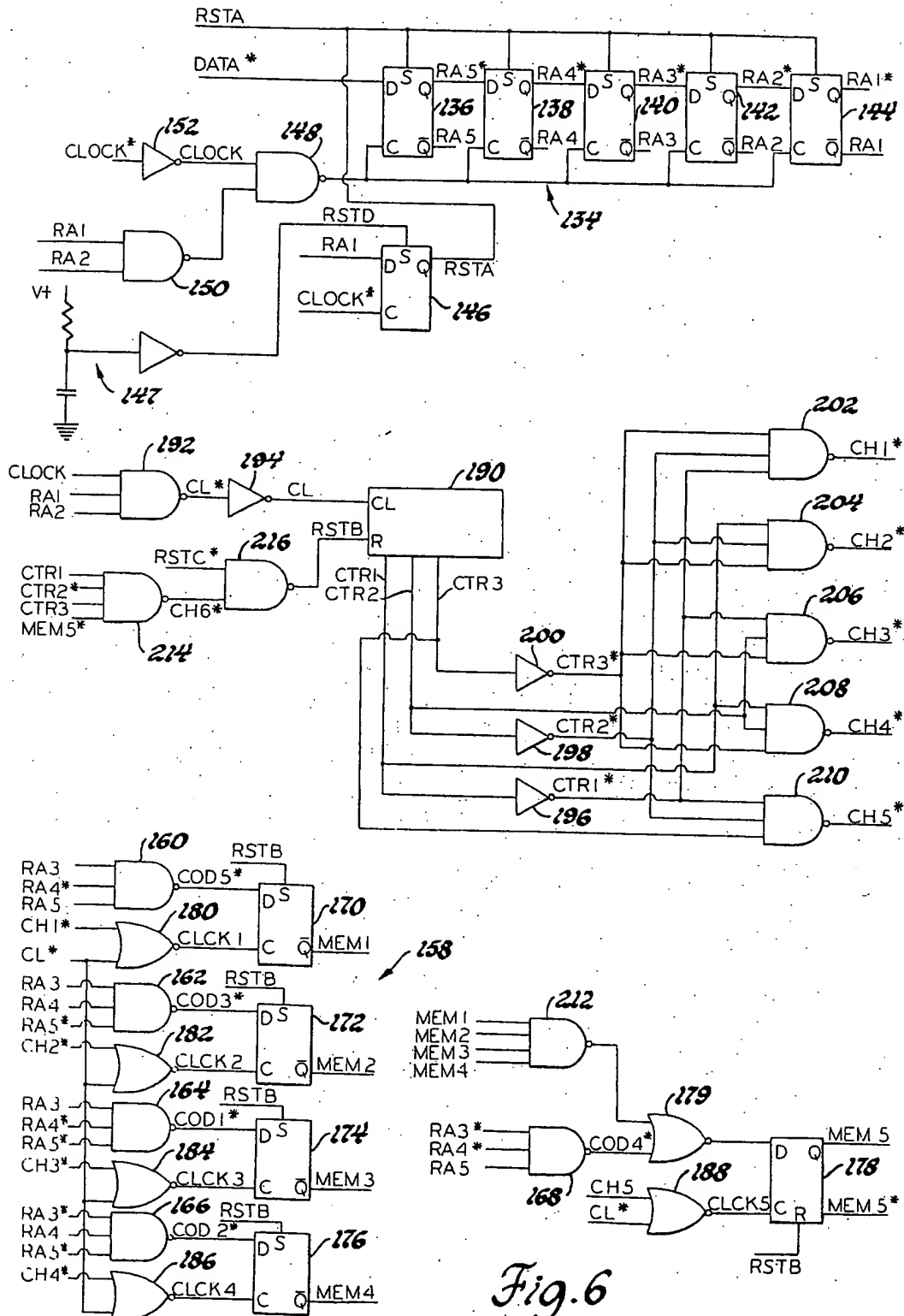


Fig. 6

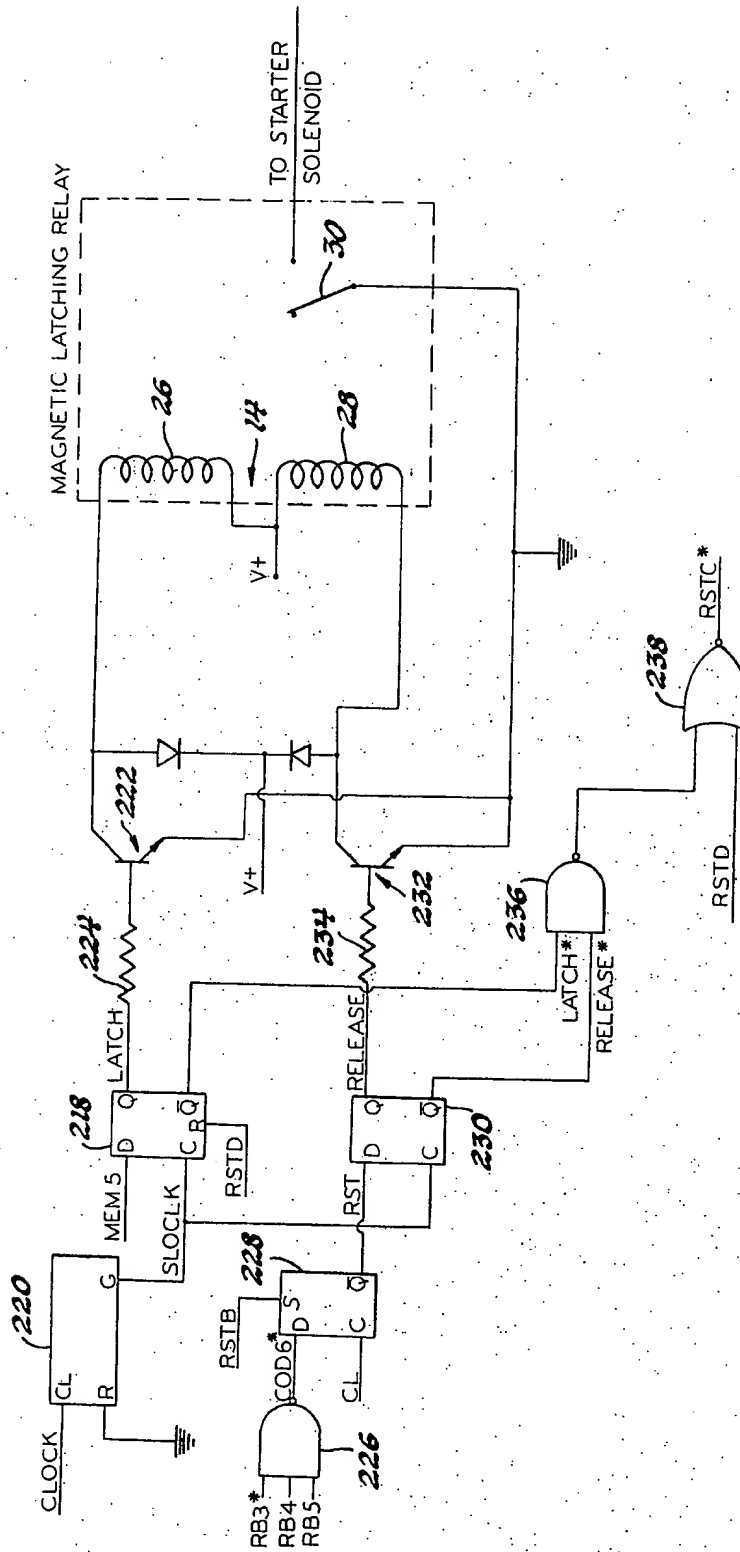
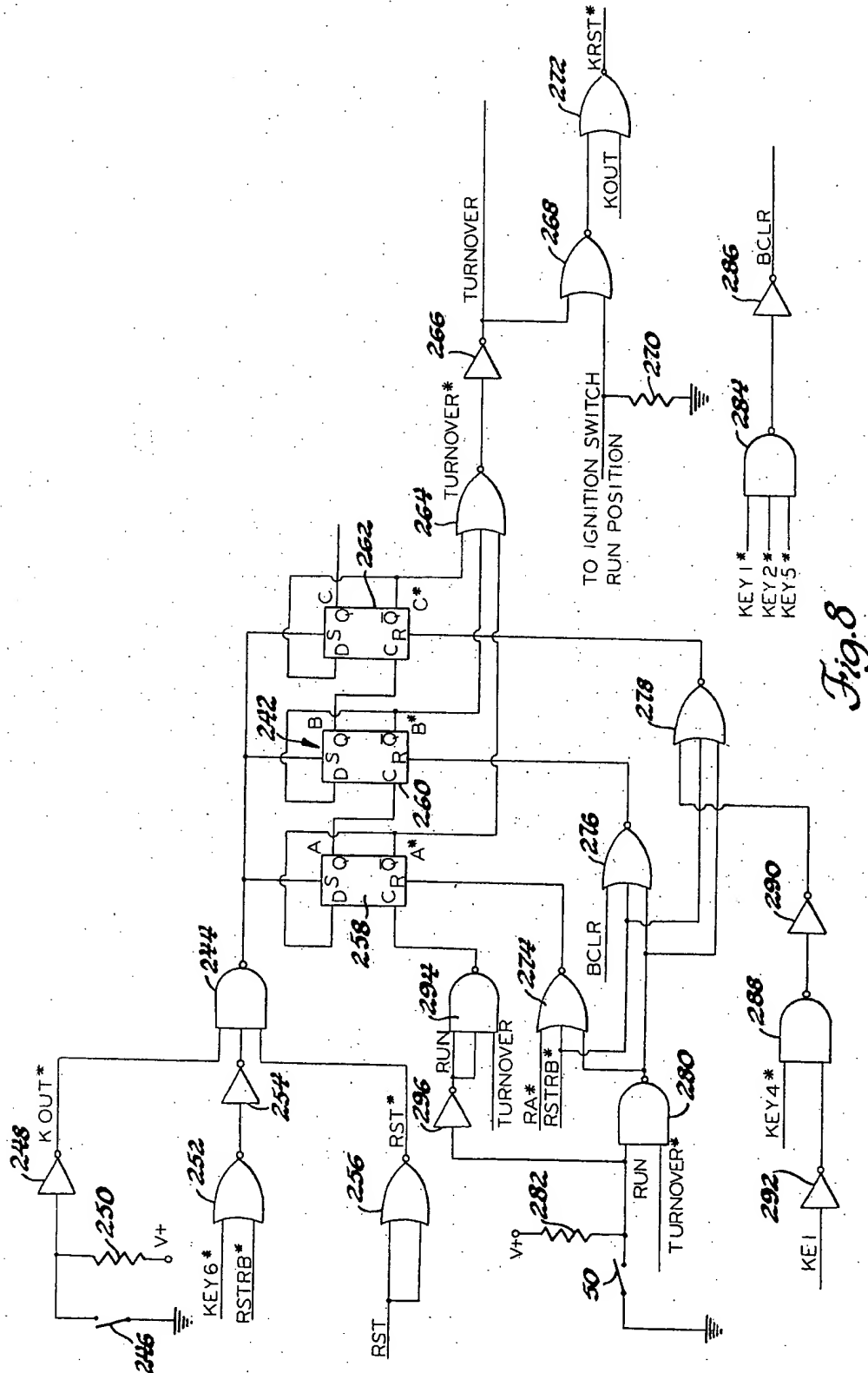


Fig. 7



## ANTI-THEFT APPARATUS INCLUDING TURNOVER MODE OF OPERATION

This invention relates to a system for inhibiting motor vehicle operation by unauthorized persons and more particularly to a system for preventing starting of a motor vehicle until the operator has entered a predetermined code into the system.

It is an object of the present invention to provide an improved anti-theft system for preventing unauthorized operation of a motor vehicle.

It is another object of the present invention to provide such a system wherein knowledge of a particular code is normally required to start the motor vehicle but wherein one who has knowledge of the code may permit others a limited number of starts of the vehicle engine without the necessity for disclosing the code.

It is another object of the present invention to provide electronic combination lock circuitry including a turnover mode of operation which permits another operator a limited number of engine starts as selected by the owner of the vehicle without the necessity for disclosing the code and wherein the turnover mode is terminated in response to removal of the ignition key.

It is a further object of the present invention to provide an anti-theft system including a keyboard unit for entering a particular combination of numbers and means for serially transmitting the data entered to a receiver unit located in a comparatively inaccessible location of the vehicle to thereby render difficult and time consuming any attempt to defeat the system.

It is another object of the present invention to provide electronic combination lock circuitry requiring the entering of a particular code in order to start the vehicle but which permits restarting of the vehicle without the necessity for entering the code as long as the ignition switch remains in the On position.

In accordance with the present invention the ground path of the starter solenoid circuit on the motor vehicle is controlled by a latching relay which is latched, to close the solenoid circuit, by combination lock circuitry responsive to operator actuation of a plurality of pushbuttons in a predetermined sequence. The lock circuitry includes a keyboard unit through which the combination code number may be entered. The digits of the number are encoded and serially transmitted to a receiver and decoder located in a relatively inaccessible part of the vehicle. If the correct code number is transmitted the latching relay is latched to permit starting of the vehicle. If the code number is not entered correctly the latching relay is released or if after the correct code is entered the ignition key is turned off the latching relay is released. If while the engine is running the operator actuates one of the numbered pushbuttons the system is placed in a turnover mode which permits the vehicle to be restarted for a number of times corresponding to the pushbutton depressed. If at any time while the vehicle is in the turnover mode the ignition key is removed, the latching relay is released to return the system to the normal mode of operation.

Other objects and advantages of the present invention will be apparent from the following detailed description which should be taken in conjunction with the drawings in which:

FIG. 1 is a schematic diagram of the system of the present invention;

FIG. 2 is a block diagram of the combination lock circuitry of the present invention; and

FIGS. 3 through 8 are more detailed logic diagrams of the lock circuitry of FIG. 2.

Referring now to the drawings and initially to FIG. 1, the anti-theft system of the present invention is generally designated 10 and comprises logic control circuitry 12 and a latching relay 14. The control circuitry 12 is connected with a source of direct current potential such as the vehicle battery 16 through a conductor 18. The conventional vehicle ignition switch generally designated 20 has one side connected with the battery 16 and is movable from a normally open position as shown to engage a Run contact connecting the ignition system with the battery 16 and is further movable to engage a Start contact connecting the starter solenoid 22 of the vehicle to the battery 16 while maintaining engagement with the Run contact. As usual, the ignition switch 20 is biased to return from the Start position to the Run position. The position of the ignition switch 20 is sensed by the control circuitry 12 through a conductor 24. The latching relay 14 includes a latch winding 26 and a release winding 28 which controls a relay contact 30 to respectively close and open the starter solenoid circuit.

Referring now to FIG. 2, the anti-theft system 10 is shown in block diagram form and includes a master unit located within the vehicle compartment, preferably on the dashboard and a remote unit located in a relatively inaccessible area such as within the starter motor enclosure. The master unit comprises a keyboard unit 32 having a plurality of operator actuable pushbuttons bearing the numerals 1 through 5 and the legend RESET. The particular combination code number is entered by the operator through the keyboard unit 32. The six pushbuttons on the keyboard unit 32 are connected with keyboard filter logic 34 which is in turn connected with a keyboard encode and transmit block 36 which encodes the digits entered through the keyboard unit 32 and serially transmits such data through a conductor 38 along with a clock signal through a conductor 40 to the remote unit generally designated 41. The remote unit 41 includes a receive and decode block 42 where the data is received and decoded and fed to a lock code memory and control logic block 44 which provides either the latch or a release signal to the latching relay 14. The starter solenoid 22 is energizable from the ignition switch 20 and controls the usual engine starter motor (not shown) of the vehicle. The master unit further includes mode logic generally designated 46 which senses the position of the ignition switch 20 as well as whether the ignition key is inserted in or has been removed from the usual ignition lock on the vehicle. A turnover logic block generally designated 48 receives an input from a condition responsive switch 50 which responds, for example, to engine manifold vacuum so as to be indicative of whether the engine is running or not. The logic block 48 also receives inputs from the keyboard encode and transmit block 36 and provides an output designated TURNOVER to the mode logic 46. The logic 48 when placed in the TURNOVER mode by the vehicle owner permits the starter relay 22 to be energized from the ignition switch 20 through the mode logic 46 for a particular number of starts without the necessity for entering the particular combination code number through the keyboard unit 32. The mode logic 46 provides a reset output to the keyboard encode and transmit unit 36 whenever the number of starts in the turnover mode have

been completed or whenever the ignition switch 20 is removed from the ignition lock.

Referring now to FIG. 3, the overall timing for the system of FIG. 2 is provided from a basic clock oscillator 52 which produces, for example, a 20 KHZ square wave output signal to the clock input of a counter 54. A reset input, designated RST, to the counter 54 is provided from an initialization circuit generally designated 56 which produces a reset pulse upon connection of the logic control circuitry with the battery 16. The circuit 56 comprises a resistor 58 and capacitor 60 with an inverter 62 connected to the junction between the resistor 58 and capacitor 60 so that a pulse with a positive going leading edge is generated upon connection with the battery 16. RST will then go low upon charging of the capacitor 60 above the threshold of the inverter 62. The counter 54 is a divide-by-128 counter producing seven successively lower frequency outputs designated TP1 through TP7. TP2 through TP7 go low upon charging of the capacitor 60 above the threshold of the inverter 62, and are inverted by the inverters generally designated 64 to produce the outputs TP2\* through TP7\*. TP3 and TP2\* provide inputs to a NOR gate 66 which produces an output designated CPB which is inverted by an inverter 67 to produce an output designated CPB\*. TP3\* and TP2\* provide inputs to a NOR gate 68 which produces an output designated CPA which is inverted by inverter 69 to produce the output designated CLOCK\*.

Referring now to FIG. 4, the individual pushbuttons 1 through 5 and RESET of the keyboard unit 32 control switches designated K1 through K6 respectively, each of which had one side grounded and the other side connected to V+ through pull-up resistors generally designated 70. The high side of the switches K1 through K6 respectively, are designated Key 1\* through Key 6\* and are connected with the keyboard filter logic 34. Referring now to FIG. 5, the filter logic 34 comprises NAND gates 72 and 74 and a NOR gate 76 which produces an output designated Key\* which is normally high but goes low in response to actuation of any of the switches K1 through K6 and returns high upon release of the switch. Key\* is connected with the D input on the first stage of a three stage counter comprising D type flip-flops 78, 80 and 82. The Q outputs of the flip-flops 78 and 80 designated K1\* and K2\* are connected with the D inputs of the flip-flops 80 and 82 respectively. The flip-flops 78, 80 and 82 are set from the initialization circuit 56 so that K1\*, K2\* and K3\* are high. The flip-flops 78 through 80 and 82 are clocked from the TP7\* output of the counter 54.

The keyboard encode and transmit unit 36 comprises binary encoding circuitry generally designated 84 the output of which is strobed into a register generally designated 86 under the control of strobe circuitry generally designated 88. The binary encoding circuitry 84 includes NAND gates 90, 92 and 94 which are connected with the pushbutton switches K1 through K6 as indicated. The output of each of the gates 90 through 94 is inverted by inverters 96, 98 and 100 and provide one input to NOR gates 102, 104 and 106. The other input to the gates 102 through 106 is provided from the strobe circuitry 88 which comprises NOR gates 108, 110 and 112 connected with the three stage counter and with the timing circuitry of FIG. 3 as indicated. The outputs of the NOR gates 108 through 112 provide inputs to a NAND gate 114 the output of which is desig-

gnated RSTRB\* which provides the other input to the NOR gates 102 through 106. The output of the gates 102 through 106 are connected with the set inputs of the first three stages of the register 86 while the output of the gate 114 is inverted by an inverter 116 and applied to the set input of the last two stages of the register 86. The register 86 comprises D type flip-flops 118 through 126 which are clocked from the output, designated REG/C, of a NAND gate 128 having its inputs connected to TP7 and CPB. The flip-flops 118 through 126 are reset to an initial condition from RST wherein their Q outputs REG1 through REG5 are low. The output of the flip-flop 126 provides one input to a NAND gate 130, the other input of which is designated Run\* and is high to open the gate 130 whenever the engine is not running. The output of the gate 130 is designated Data\*.

Briefly, the operation of the circuitry thus far described is as follows: Depression of one of the switches K1 through K6 causes the binary equivalent of the corresponding digit to be entered in the flip-flops 118, 120 and 122 of the register 86 when RSTRB\* goes low. At the time the flip-flops 124 and 126 of the register 86 are set high from RSTRB. Consequently, as the data is shifted out of the register 86 by the clock pulses REG/C the data is always preceded by two logic "1's" for identification purposes.

Referring now to FIG. 6, the receive and decode logic block 42 comprises a data register generally designated 134 which includes D type flip-flops 136 through 144. The flip-flops 136 through 144 are set so that their Q outputs are high by a reset signal designated RSTA. RSTA is derived from the Q output of a flip-flop 146 which is initially set high from an initialization circuit 147 which is identical to the circuit 56. The circuit 147 produces a pulse designated RSTD when the logic circuitry is first connected with the vehicle battery. Thereafter, the flip-flop 146 is toggled and the register 134 is set by the rising edge of CLOCK\* whenever the Q output of the flip-flop 144, designated RA1, is high. The data is shifted into the register 134 by a NAND gate 148 having its output connected to the clock input of each of the flip-flops 136 through 144. One input to the gate 148 is from a NAND gate 150 which has inputs connected to the Q outputs of the flip-flops 142 and 144, designated RA2 and RA1 respectively, which go low when the register 134 is set. The other input to the gate 148 is from CLOCK\* which is inverted by an inverter 152 the output of which is designated CLOCK. The gate 148 is open whenever the register 134 is set so that the data is shifted into the register on the following edge of CLOCK until the first two bits, which are logic "1's," are entered in the flip-flops 142 and 144, whereupon RA1 and RA2 go high and the gate 148 is closed.

The register 134 stores the data for a one CLOCK pulse interval and thereafter the register 134 is set from the flip-flop 146. During this one CLOCK pulse interval the data stored in the register 134 is decoded.

The outputs of the flip-flops 136 through 144 in the register 134 are connected with decode logic generally designated 158 which comprises NAND gates 160 through 168 connected with the outputs of the flip-flops 136 through 144 in the register 134 as indicated. The decode logic 158 is hard wired with the register 134 to decode the particular combination code number which in the example shown is 53124. The outputs of

the gates 160 through 166 are connected with the D input of flip-flops 170 through 176 respectively while the output of the gate 168 is connected to the D input of flip-flop 178 through a NOR gate 179. The flip-flops 170 through 178 are clocked through NOR gates 180 through 188 which are open in sequence to insure that the five numbers of the code are inserted in the keyboard unit 32 in the proper sequence. The  $\bar{Q}$  outputs of the flip-flops 170 through 176 and the Q output of the flip-flop 178 are designated MEM1 through MEM5 respectively. The  $\bar{Q}$  output of the flip-flop 178 is designated MEM5\*. The sequential control of the gates 180 through 188 is controlled from a BCD counter 190 which is advanced on the rising edge of CLOCK through a NAND gate 192 and an inverter 194. The other inputs to the gate 192 besides CLOCK are RA1 and RA2 so that the gate 192 is opened for the CLOCK pulse interval following the entering of the binary data in the register 134. In other words, after CLOCK goes low to enter the most significant bit in flip-flop 136, the gate 148 is closed and the gate 192 is opened. On the following rising edge of CLOCK, CL\* goes low and CL goes high and the counter 190 is incremented and on the following falling edge of CLOCK, i.e. CLOCK\* goes high, the flip-flop 146 is toggled causing RSTA to go high and reset the register 134. When the register 134 is reset the gate 148 is opened and the gate 192 is closed. The outputs of the counter 190 designated CTR1 through CTR3 are inverted by inverters 196, 198 and 200 to provide the outputs designated CTR1\* through CTR3\* respectively. CTR1 through CTR3 and CTR1\* through CTR3\* are connected with NAND gates 202 through 210 as indicated. The outputs of the gates 202 through 210 are designated CH1\* through CH5\* respectively. The counter 190 is reset from RSTC\* through a NAND gate 216, the output of which is designated RSTB, or from a NAND gate 214. The input to the gate 214 is the CTR1, CTR2\*, CTR3 outputs of counter 190 and the MEM5\* output of the flip-flop 178. The RSTC\* input to gate 216, as will be shown hereinafter, goes low and RSTB goes high when RSTD goes high to initially reset the counter 190. When RSTB goes high the flip-flops 170 through 176 are set to drive MEM1 through MEM4 low and the flip-flop 178 is reset to drive MEM5 low and MEM5\* high. With the counter 190 reset CH1\* is low and CH2\* through CH5\* are high. Accordingly, when CL\* goes low, just prior to incrementing the counter 190, the flip-flop 170 will be toggled to cause MEM1 to go high if the pushbutton switch K5 had been depressed since in that event RA3, RA4\* and RA5 would be high. As the counter 190 is incremented CH2\* goes low and the next binary coded number entered through the keyboard unit 32 is decoded by the gate 162. If the number 3 is entered MEM2 is toggled high on the falling edge of CL\*. Similarly, MEM3 and MEM4 go high if the pushbutton switches K1 and K2 are successfully depressed. The four outputs of the flip-flops 170 through 176 are inputs to a NAND gate 212, the output of which is connected with the NOR gate 179 so that if the first four numbers of the code are entered and in the proper sequence and the pushbutton switch K4 is thereafter depressed, the outputs of the flip-flop 178 designated MEM5 is toggled high and MEM5\* is toggled low.

Referring now to FIG. 7, MEM5 is connected to the D input of a flip-flop 218 which is initially reset from

the RSTD output of the initialization circuit 147. The flip-flop 218 is clocked from the output of a BCD counter 220, designated SLOCLK, which is driven from and is at a frequency of, for example, 20 Hz. as compared with the CLOCK frequency of, for example, 2KHz. When the flip-flop 218 is clocked while MEM5 is high its Q output designated LATCH goes high. The Q output of the flip-flop 218 is connected with the base of a transistor 222 through a resistor 224. The emitter electrode of the transistor 222 is grounded while its collector is connected to V+ through the latch winding 26 of the latching relay 14. Accordingly, if the correct combination is entered through the keyboard unit 32 the latch winding 26 is energized and its contact 30 is moved from the position shown to provide a ground path for the starter 22 solenoid.

If the reset button K6 of FIG. 4 is depressed the binary equivalent of the numeral 6 is transmitted to the register 134 causing the inputs to a NAND gate 226 to go high and the output thereof designated COD6\* to go low. The output of the NAND gate 226 is connected to the D input of a D type flip-flop 228 which is toggled from CL. Accordingly, on the rising edge of CL (FIG. 6) following depression of the reset pushbutton switch K6, the  $\bar{Q}$  output of the flip-flop 228 designated RST goes high. RST is connected with the D input of a D type flip-flop 230 which is clocked from SLOCLK and has its Q output designated RELEASE connected to the base of a transistor 232 through a resistor 234. The emitter of the transistor 232 is grounded while the collector is connected to V+ through the release winding 28 of the latching relay 14. Accordingly, the release winding 28 may be energized to open the ground path of the starter solenoid 22 by actuating the reset pushbutton switch K6. The  $\bar{Q}$  outputs of the flip-flops 218 and 230 designated LATCH\* and RELEASE\* respectively are inputs to a NAND gate 236 the output of which is connected with a NOR gate 238. The other input to the NOR gate 238 is RSTD from the initialization circuit 147. The output of the gate 238 is the previously mentioned RSTC\* which provides the other input to gate 216 of FIG. 6. Thus, whenever the latching relay 14 is either latched or released RSTC\* goes low to reset the counter 190 and the flip-flops 178 and set the flip-flops 170 to 176 and 228.

If the code number is incorrectly entered MEM5\* will remain high and after the fifth pushbutton switch has been actuated CTR1, CTR2\* and CTR3 will be high so the output of the gate 214 will go low and RSTB will go high to reset the counter 190 and the memory flip-flops and release the latching relay 14.

Referring now to FIG. 8, the turnover logic 48 is disclosed in greater detail. The turnover logic 48 permits the owner of the vehicle or anyone else having knowledge of the combination to turn over limited use of the vehicle to one not having knowledge of the combination without the necessity of disclosing the combination. Use is limited by the operator prescribing the number of vehicle starts to be permitted. The logic 48 comprises a three stage counter 242 which is set through a NAND gate 244 which performs an OR function. One input to the gate 244 is K OUT\* which is derived from a switch 246 which closes when the ignition key is placed in the ignition lock and opens when the ignition key is removed from the ignition lock. One side of the switch 246 is grounded while the other side is connected with an inverter 248 which is tied to V+

through a pull-up resistor 250. Another input to the gate 244 is from the reset pushbutton switch K6 and the accompanying RSTRB\* through a NOR gate 252 and an inverter 254. The other input to the NAND gate 244 is from the initialization circuit 56 through a NOR gate 256. The counter 242 comprises flip-flops 258, 260 and 262. The flip-flops 258, 260 and 262 are initially set from RST so that their Q outputs are high and their  $\bar{Q}$  outputs are low. The  $\bar{Q}$  outputs of the flip-flops 258 through 262 provide inputs to a NOR gate 264, the output of which is designated TURNOVER\*, which is inverted by an inverter 266 to provide the output designated TURNOVER. Thus, initially the output of the gate 264 is high and the output of the inverter 266 is low indicating that the vehicle is not in the turnover mode. If at any time the ignition key is removed from the ignition lock or the reset pushbutton switch K6 is actuated the counter 242 is set so that the output of the inverter 266 goes low. The output of the inverter 266 provides one input to a NOR gate 268. The other input to the NOR gate 268 is tied to ground through a pull down resistor 270 and is also connected with the Run position of the ignition switch 20. The output of the gate 268 provides one input to a NOR gate 272 the other input of which is K OUT. The output of the gate 272 is designated KRST\* and provides one input to the gates 92 and 94 of the encoding circuitry 84 (FIG. 5). Thus, if KRST\* goes low the binary equivalent of the reset pushbutton switch K6 is transmitted to the receive and decode unit 42 to release the latching relay 14. KRST\* will go low if the ignition key is removed from the ignition lock or, if the vehicle is not in the turnover mode and the ignition switch is turned off. The flip-flops 258, 260 and 262 are programmed by encoding logic comprising NOR gates 274, 276 and 278. The NOR gates 274, 276 and 278 are each controlled from a NAND gate 280. One input to the gate 280 is TURNOVER\*. The other input to the gate 280 is from the engine manifold vacuum switch 50 or other appropriate engine run conditioning sensor and also to V+ through a pull up resistor 282. Thus, the gates 274, 276 and 278 are closed if the engine is not running or the system is in the turnover mode. In other words, the counter 242 can be programmed for a particular number of free starts only if the engine is running and the system is not already in the turnover mode. The second input to each of the gates 274, 276 and 278 is from RSTRB\* which goes low in response to actuation of any of the pushbutton switches K1 through K6. The third input to the gate 274 is from RA\* (FIG. 5) which goes low in response to actuation of either of the pushbutton switches K1, K3 or K5. The third input to NOR gate 276 is designated BCLR and is derived from the output of a NAND gate 284 through an inverter 286. The inputs to the gate 284 are KEY1\*, KEY2\*, and KEY5\*. Accordingly, BCLR goes low if either of the pushbutton switches K1, K2 or K5 is actuated. The third input to the NOR gate 278 is derived from a NAND gate 288 through an inverter 290. The inputs to the NAND gate 288 are KEY4\*, and KEY1 (FIG. 5) through an inverter 292. Accordingly, the output of the inverter 290 goes low if either of the pushbutton switches K1, K2, K3 or K4 is actuated. Thus, the  $\bar{Q}$  outputs of the flip-flops 258, 260 and 262 will be reset to the binary equivalent of any pushbutton switch depressed while the vehicle is running and the vehicle is not in the turnover mode. For example, if the register 242 is set so that

TURNOVER\* is high and if the engine is running and the driver depresses the pushbutton switch K4, the  $\bar{Q}$  output of the flip-flop 262 will be reset high and the  $\bar{Q}$  outputs of the flip-flops 258 and 260 will remain low. When the  $\bar{Q}$  output of the flip-flop 262 goes high TURNOVER\* goes low closing the gate 280. TURNOVER\* will remain low until the counter 242 has been toggled four times. The counter 242 is toggled through a NAND gate 294 and inverter 296 each time the switch 50 opens while TURNOVER is high. Thus, each time the engine is started during the turnover mode the counter 242 is toggled so that after four starts, all inputs to the gate 264 are low and TURNOVER goes low. Accordingly, when the ignition switch 20 is turned off after the fourth start the output of the gate 268 goes high and KRST\* goes low to generate the reset number 6 and interrupt the circuit to the starter solenoid 22.

Having thus described my invention what I claim is:

1. In a motor vehicle provided with starter motor control means for controlling starting of the vehicle engine, including an ignition switch operable by an ignition key, apparatus for preventing unauthorized starting of said vehicle comprising:

a keyboard unit including a plurality of operator actuable switch means;

latch means for enabling said starter motor control means;

latch control means responsive to actuation of said switch means in a predetermined sequence for energizing said latch means to enable said starting motor control means;

said latch control means responsive to actuation of said ignition switch to an off position for releasing said latch means to disable said starter motor control means;

override means for overriding said ignition switch and thereby prevent releasing of said latch means, said override means including counter means, means responsive to actuation of one of said switch means while said vehicle engine is running to program said counter means to a predetermined number of ignition switch actuations, said counter means being advanced each time said engine is started after said counter means is programmed whereby the override condition is terminated after said engine has been started said predetermined number of times;

and means responsive to removal of said ignition key for resetting said counter means.

2. In a motor vehicle provided with an electrical load device for controlling usage of the vehicle, apparatus for preventing unauthorized usage of said vehicle comprising:

input means including a plurality of operator actuable switch means;

latch means for enabling said load device;

latch control means responsive to actuation of said switch means in a predetermined sequence for energizing said latch means to enable said load device;

an additional operator actuable switch means;

said latch control means responsive to actuation of said additional switch means for releasing said latch means to disable said load device;

override means for overriding said additional operator actuable switch means and thereby preventing release of said latch means, said override means in-

3,784,839

9

cluding counter means, means responsive to actuation to one of said plurality of operator actuatable switch means while said load device is enabled to program said counter means to a predetermined number of actuations of said additional operator- 5 actuatable switch means, said counter means being

10

advanced each time said additional switch means is actuated after said counter means is programmed whereby the override condition is terminated after said additional switch means has been actuated said predetermined number of actuations.

\* \* \* \* \*

10

15

20

25

30

35

40

45

50

55

60

65



[54] MANUALLY SET MAGNETIC RELAY

[75] Inventor: Charles D. Flanagan, Attleboro, Mass.

[73] Assignee: Texas Instruments Incorporated, Dallas, Tex.

[22] Filed: Dec. 5, 1973

[21] Appl. No.: 421,903

[52] U.S. Cl. .... 335/186, 123/179, 180/82 C, 335/164, 340/52 E

[51] Int. Cl. .... H01h 45/00

[58] Field of Search ..... 335/186, 166, 167, 171, 335/164, 165, 160, 159; 340/52 E, 278; 180/82 C, 96; 307/114, 10 AT, 10 SB; 200/61.58 B; 123/179 R, 179 B

[56] References Cited  
UNITED STATES PATENTS

2,361,564 10/1944 Platz ..... 335/164  
3,449,714 6/1969 Farley, Jr. .... 340/52 E

Primary Examiner—Harold Broome

Attorney, Agent, or Firm—John A. Haug; James P. McAndrews

[57]

ABSTRACT

A manually set magnetic relay is utilized to override an electrical interlock in a one-time operation. Once the relay has been utilized, it automatically disables itself and must be manually set again for another operation. The relay includes an electromagnetic coil which closes a load switch connected in parallel with the electrical interlock. A secondary circuit for energizing the coil includes a second switch formed by a pair of flexible conductors at least one being flexible. A flexible latch engages one of the conductors of the second switch as the coil is energized and closes the load switch. The latch continues to hold the second switch in the latched and open condition when the coil is de-energized. To close the second switch and make energization of the coil possible, a manually actuated plunger engages the flexible latch and displaces it away from the one of the flexible conductors which then moves from the latched position to a position in contact with the other conductor of the second switch. The plunger also holds the load switch open during the unlatching operation to provide trip-free operation of the relay.

6 Claims, 5 Drawing Figures

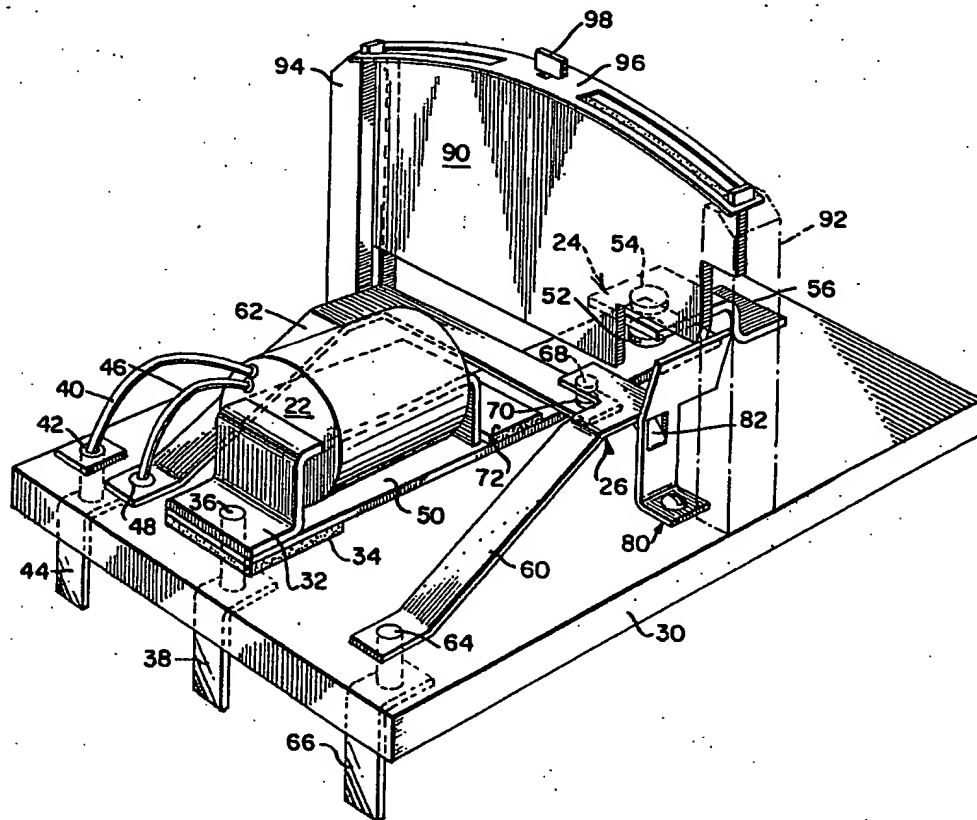


FIG. 1

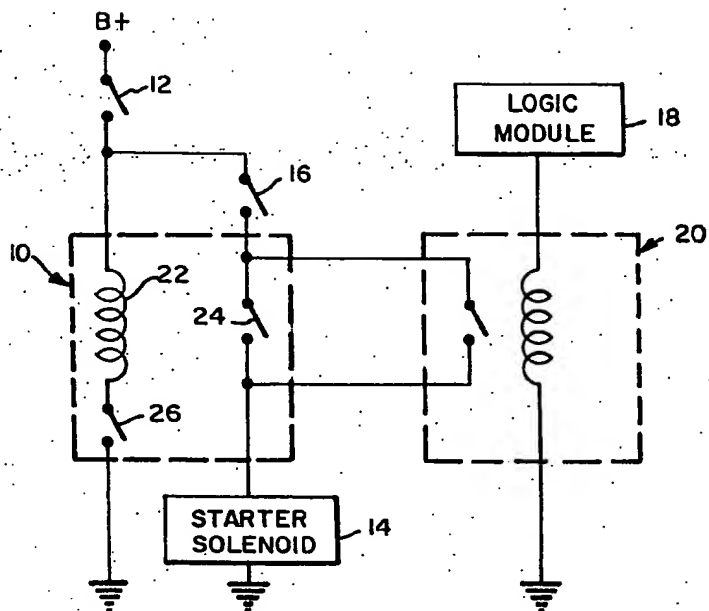
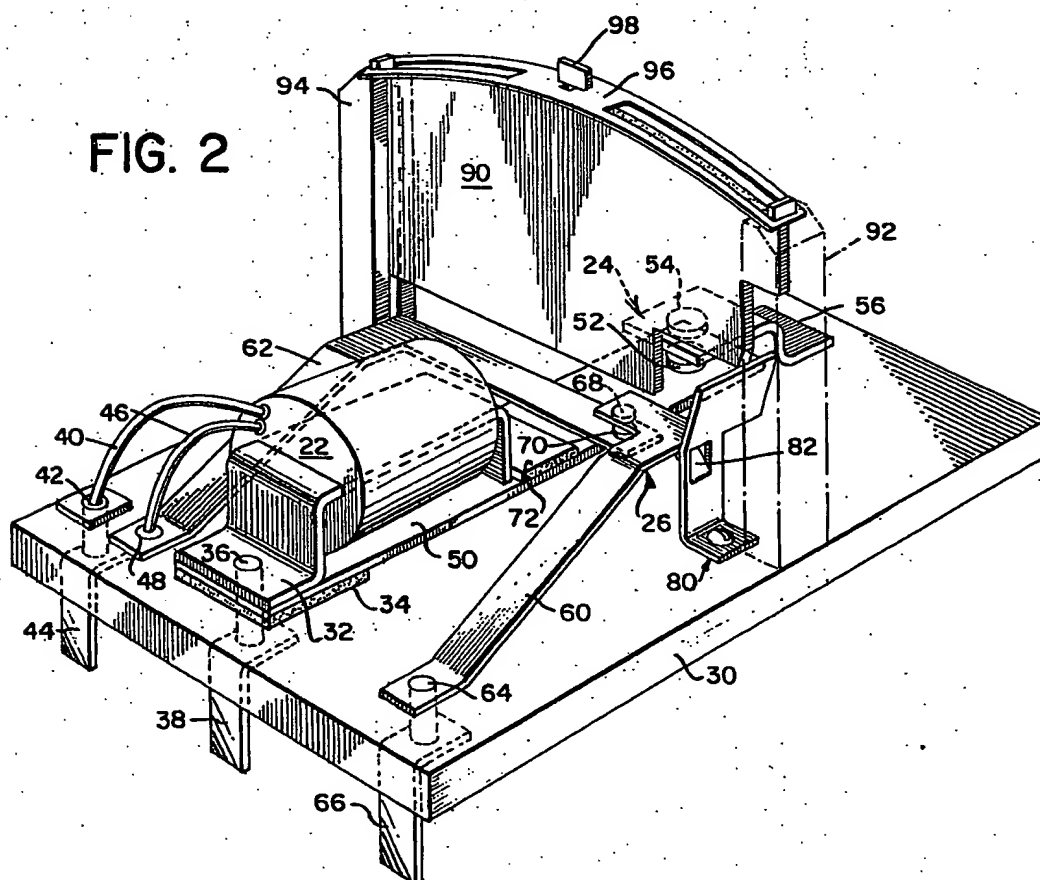


FIG. 2



PATENTED FEB 4 1975

3,864,651

SHEET 2 OF 2

FIG. 3

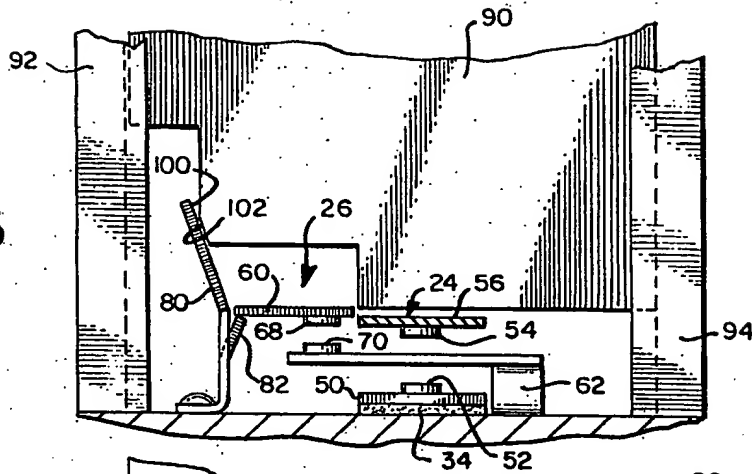


FIG. 4

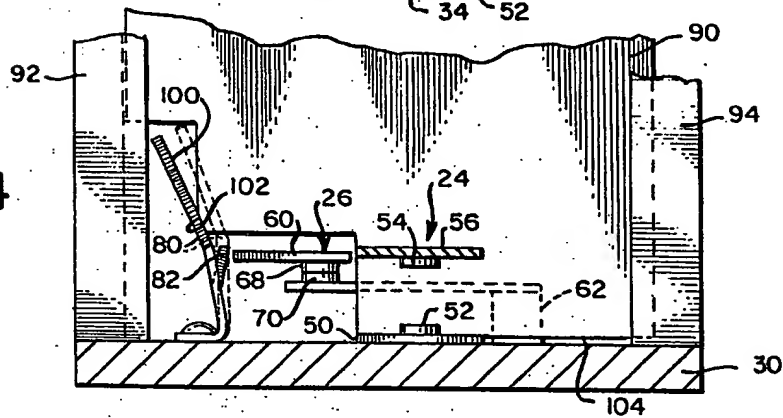
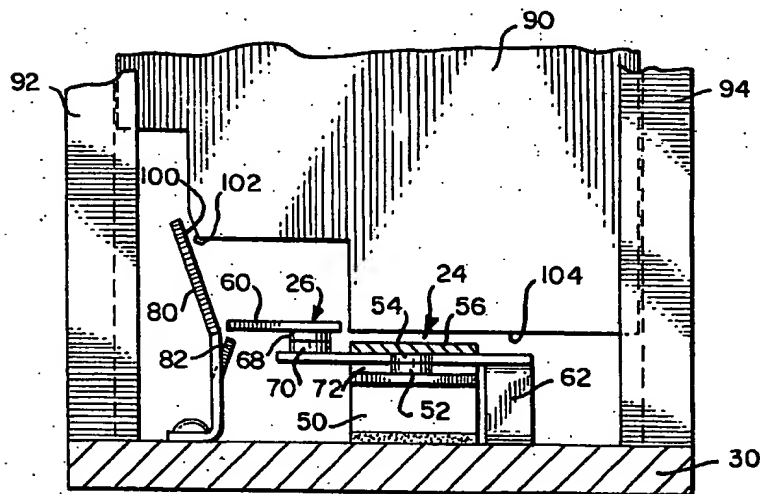


FIG. 5



## MANUALLY SET MAGNETIC RELAY

### CROSS-REFERENCE TO RELATED APPLICATIONS

This application relates to subject matter disclosed and claimed in copending application Ser. No. 421,889 entitled, "Manually Set Switching Devices" filed Dec. 5, 1973, and copending application Ser. No. 421,902, entitled "Manually Set Magnetic Relay", filed Dec. 5, 1973, and copending application Ser. No. 421,904, entitled "Push Button", filed Dec. 5, 1973, the copending applications having the same assignee as the present application.

### BACKGROUND OF THE INVENTION

This invention relates to the field of electrical relays and, more particularly, is related to a single-cycle magnetic relay which must be manually set in an enabled condition prior to each operation.

It is well known to provide electrical interlocks in systems to prevent operation unless specific conditions have been met. For example, as a safety measure in automobiles, the ignition system may be disabled until the driver and all of his passengers have fastened their seat belts. To implement such a system, an electrical interlock operated by sensors or switches sequentially set by the driver and passengers entering the car and fastening the belts may be provided in the ignition system of the automobile. Unless the belts are fastened after entry, the interlock disables the ignition system and the engine cannot be started.

It will be recognized that a failure of the electrical interlock system may completely disable the ignition system and prevent operation of the automobile. Such a situation may not only be frustrating to the driver and his passengers but also could prove to be a serious hazard particularly in an emergency situation in which the automobile must be moved.

To remedy the situation and eliminate the possible hazards posed by the electrical interlock, it has been suggested that an override relay be provided to bypass the electrical interlock. The relay must be manually set before each override operation and disabled after operation. Naturally, to prevent repeated use of the relay, it is located in a position not readily accessible to the driver except in an emergency situation, and one likely location for the relay is the engine compartment.

It is, accordingly, a general object of the present invention to disclose a manually set magnetic relay which automatically disables itself when de-energized to limit its use to single-cycle or one-time operations.

### SUMMARY OF THE INVENTION

The present invention resides in a manually set magnetic relay for single-cycle or one-time operations. The relay has particular utility as an overriding device for an electrical interlock since the relay must be manually set prior to each overriding operation and automatically disables itself after a single operation so that the interlock may again perform its intended function.

The magnetic relay is comprised of first switch means which are operatively connectible in the load circuit controlled by the electrical interlock. The first switch means includes a cantilevered, flexible clapper arm.

Electromotive force generating means including an electromagnetic coil is operatively connected with the clapper arm of the first switch means for closing the

first switch means upon energization of the coil. Such energization in the automobile interlock system takes place at the beginning of engine starting procedures.

Second switch means serially coupled with the coil of the electromotive force generating means permit energization of the coil and include first and the second flexible conductors having portions positioned in overlying relationship for flexing in and out of contact and thereby closing and opening the second switch. The second conductor extends in transverse relationship to the clapper arm of the first switch means and is engaged by the clapper arm for flexing in and out of contact with the first conductor of the second switch means. When the clapper arm of the first switch means closes as the relay is pulled in, the second conductor moves the first conductor into a position above a latch means which is operatively engageable with the first conductor to hold it in a latched position out of contact with the first conductor after de-energization of the electromagnetic coil. With the first conductor latched, the coil cannot be re-energized.

Unlatching of the first conductor of the second switch means to enable the relay is performed by a manually operable actuator means engaged with the latching means for releasing the conductor from the latched position. The actuator means includes a plunger having a camming surface which contacts a flexible member of the latching means and moves the member away from the first conductor to allow the first conductor to snap into contact with the second conductor and close the second switch means.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an electrical diagram illustrating one environment in which the manually set magnetic relay of the present invention may be employed.

FIG. 2 is a perspective view of the magnetic relay in its disabled condition.

FIG. 3 is an enlarged end view of the magnetic relay in FIG. 2 partially in section and illustrating the components in the disabled condition of the relay.

FIG. 4 is an end view of the relay similar to that in FIG. 3 and illustrates the components during manual actuation for setting the relay in an enabled condition.

FIG. 5 is an end view similar to FIGS. 3 and 4 and illustrates the components when the relay is pulled in.

### DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is an electrical diagram showing schematically the manually set magnetic relay of the present invention in the starting circuitry of an automobile having an electrical ignition interlock. The interlock normally prevents energization of the electrical starter motor unless the seat belts have been properly fastened in each of the occupied seats of the automobile. It should be understood, however, that the magnetic relay of the present invention can be employed in other environments to override an interlock or perform other functions to which its operation is suited.

The manually set magnetic relay of the present invention, generally designated 10, is connected serially in the electrical starting circuit between the ignition switch 12 and the starter solenoid 14 on the starter motor (not illustrated). The ignition switch 12 is, of course, connected to one of the battery terminals, the B+ terminal being illustrated, and the starter solenoid

14 would be connected to the other terminal, illustrated as the ground terminal, through the frame of the automobile. A starting switch 16 is also serially connected with the magnetic relay between the ignition switch 12 and the solenoid 14. The ignition switch 12 and the starting switch 16 are generally incorporated in a single switching device manually operated by means of the ignition key and are closed sequentially, the switch 12 being closed first and the switch 16 being closed second by rotating the ignition key through several index positions, the last of which closes the switch 16 to energize the starter solenoid 14 and turn the starter motor. Usually, the last index position is spring-biased so that the starting switch 16 opens upon release of the key. The ignition switch 12 also energizes other portions of the electrical system such as the spark coil, fuel pumps and instrumentation needed during operation of the engine.

The seat belt interlock system includes a logic module 18 and an interlock relay 20. The logic module 18 receives signals from sensing switches indicating which seats of the automobile are occupied and which seat belts have been fastened. If the seats are first occupied and then the respective seat belts are fastened in that order, a "go" signal normally issues from the module 18 to actuate the coil of the interlock relay 20 and close the relay contacts. The relay contacts in the closed position complete the starting circuit through the switches 12 and 16 to the starter solenoid 14 and permit the starter motor to be engaged. If the logic module detects an unfastened seat belt in one of the occupied seats, or if the sensing switches are not actuated in the proper order, indicating, for example, a permanently buckled seat belt, the interlock relay 20 is not energized and the starting circuit remains open. Also, however, if the logic module 18 is faulty and inoperative, the interlock contacts may not close and starting the automobile cannot take place in its intended fashion.

The manually set magnetic relay 10 is employed in parallel with the interlock relay 20 to override the interlock when it is inoperative for any reason and therefore permits the automobile to be started. The magnetic relay 10 is comprised of electrical components including an electromagnetic relay coil 22, a load switch 24 operated by the coil and a latching switch 26 in a secondary circuit with the coil. The contacts of the load switch 24 are connected in parallel with the contacts of the interlock relay 20 so that they may duplicate or override the relay 20 when the interlock system fails. In order to close the load switch 24, however, the latching switch 26 must be closed and the magnetic coil 22 must be energized through the ignition switch 12. The latching switch 26, as described in greater detail below, must be manually set to the closed position and is automatically opened to disable the relay 10 when the coil 22 is de-energized after the ignition switch 12 is opened to shut off the automobile engine. Hence, the magnetic relay 10 provides a single-cycle override or bypass operation of the seat belt interlock system for each operation of the automobile engine. It will be understood that the manually set magnetic relay 10 would be located in a position not readily accessible to the driver of the automobile, for example, in the engine compartment, so that the seat belt interlock system is not routinely overridden.

FIG. 2 illustrates a construction and the principal components of the manually set magnetic relay 10. The

principal components of the relay including the coil 22, the load switch 24 and the latching switch 26 are all supported on a base plate 30 formed preferably from an insulating material such as a plastic or fiberboard.

The electromagnetic coil 22 includes a U-shaped ferromagnetic support bracket 32 around which the coil 22 is wound. The bracket 32 is fixedly riveted to a platform 34 on the base plate 30 by means of a terminal post 36. A connecting pin 38 is attached to the lower end of the post 36 for plugging the relay into an electrical connector. One lead 40 from the coil 22 is connected to a terminal post 42 extending through the base plate 30 to a connecting pin 44. The other lead 46 from the coil 22 is connected to a terminal post 48 on the base plate.

The U-shaped bracket 32 is mounted on the platform 34 in cantilever fashion so that the free end of the bracket is located over a resilient and conductive clapper arm 50. The clapper arm 50, like the bracket 32, is mounted in cantilever fashion between the platform 34 and the bracket and is held by the terminal post 36. In the unflexed condition, the clapper arm 50 extends generally parallel to the upper surface of the base plate 30 and a small gap exists between the clapper arm and the free end of the bracket 32. It will be readily understood that energization of the coil 22 generates magnetic flux through the ferromagnetic bracket 32 and the conductive and ferromagnetic clapper arm 50 and pulls the clapper arm upwardly against the free end of the bracket 32 to close the gap. Clapper arm 50 may also be a composite of an electrically conductive but non-ferromagnetic arm and a ferromagnetic section in operable engagement therewith between the fixed and the free end of the bracket 32.

The resilient and conductive clapper arm 50 includes at its free end an electrical contact 52 and thus forms a part of the load switch 24. The other electrical contact 64 of the load switch 24 is supported directly above the contact 52 on a bracket 56 attached to the base plate 30 by a terminal post (not shown) so that the contacts 52 and 54 meet when the clapper arm 50 is pulled upwardly by the electromagnetic coil 22. A connecting pin (not shown) similar to pins 38 and 44 is also connected to the terminal post holding the bracket 56.

The latching switch 26 in the secondary circuit controlling the coil 22 is formed by two generally flat conductors 60 and 62, as described both are resilient although it should be noted that one of the two may be rigid. The conductor 60 is riveted to the base plate 30 by means of a terminal post 64 and extends in cantilever fashion from the post over the plate 30. A connecting pin 66 similar to pins 38 and 40 is secured to the bottom end of the post below the plate 30. At the free end of the cantilevered conductor 60 is an electrical contact 88 which overlies and mates with a contact 70 on the end of the flexible conductor 62. The conductor 62 is riveted to the base plate 30 by the terminal post 48 and is in electrical contact with the lead 46 at the terminal post. The conductor 62 extends in cantilever fashion from the terminal post 68 in a direction generally parallel to the clapper 50 and then extends transversely across the clapper to the free end bearing the contact 70. An insulating pad 72 is positioned on the clapper 50 directly below the conductor 62 so that the clapper arm 50 when raised by the coil 22 lifts the conductor 62 without establishing electrical contact with the conductor. The conductor 62 in the unflexed con-

dition may be positioned as illustrated at an elevation above the base plate 30 providing space between the conductor and the insulating pad 72 when the clapper arm 50 is not pulled upwardly by the coil 22.

A resiliently flexible, one-piece latch 80 is fixed to the base plate 30 at a position laterally adjacent the free end of the flexible conductor 60. The one-piece latch 80 includes a projecting, inclined tang 82 on which the conductor 60 is shown resting in FIG. 2. The height of the tang 82 above the base plate 30 is selected in conjunction with the bracket 32, the clapper arm 50 and conductor 62 to locate the contacts 68 and 70 of switch 26 open or out of contact when the coil 22 is de-energized and the conductor 60 is resting on the tang. Furthermore, when the clapper arm 50 is elevated by the coil 22, the arm 50 lifts the conductor 60 to a position just above the latch 80 by means of the intervening conductor 62 extending transversely across the clapper arm 50 and the insulating pad 72.

A manually actuated plunger 90 is supported for reciprocation in slots of two upright guide posts 92 and 94 at opposite sides of the base plate 30. The posts 92 and 94 may be formed integrally with the base plate or separately attached to the plate. A return spring 96 extends between the tops of the posts 92 and 94 and has a central slot which captures a knob 98 at the top of the plunger 90. The plunger 90 may, therefore, be reciprocated along an axis extending parallel to the slots in the posts 92 and 94 and perpendicular to the base plate. In operation of the relay, the knob 98 and remaining portion of the plunger 90 are manually depressed toward the base plate 30 and when released, the plunger is returned to the position illustrated by the spring 96.

#### OPERATION

The operation of the manually set magnetic relay 10 and the remaining structural details of the relay are described below in connection with FIGS. 3-5 which show the relay in three different and sequential stages of operation.

FIG. 3 illustrates the positions of the relay components when the relay is in a de-energized and disabled condition. The flexible conductor 60 is held in the latched position on top of the tang 82 and the flexible conductor 62 is in an unflexed condition locating the contact 70 directly below and spaced from the contact 68. The switch 26 formed by the conductors 60 and 62 is, therefore, open, and the secondary circuit through the relay coil 22 is interrupted.

Since the circuit through the coil 22 is interrupted, it is de-energized and the resilient clapper arm 50 is located in its unflexed position spaced slightly above the base plate 30 but well below the bracket 56 so that the contacts 52 and 54 are in spaced relationship, one above the other. The load switch 24 is, accordingly, open and the electrical interlock relay 20 (FIG. 1) is free to perform its intended function of preventing engine start-up unless the logic module 18 is satisfied that the seat belts in occupied seats have been appropriately fastened.

FIG. 4 illustrates the positions of the relay components when the manually actuated plunger 90 is fully depressed to initiate an override operation. It will be observed in FIGS. 2 and 4 that the latch 80 has an extension bearing a camming surface 100 engaged by a corresponding camming surface 102 on the actuated plunger as the plunger is depressed in the slots of the

guide posts 92 and 94. The camming surfaces are disposed at a slight angle to the axis of reciprocation of the plunger. Movement of the plunger vertically toward the base plate 30 causes the camming surfaces 102 and 104 to slide relative to one another and displaces the latch 80 together with the tang 82 from the phantom position in the lateral direction generally perpendicular to the motion of the plunger along the axis of reciprocation. As the latch moves to the position illustrated in FIG. 4 from the phantom position, the tang 82 is removed from its supporting position under the resilient conductor 60 and the conductor snaps downwardly onto the conductor 62. The electrical contacts 68 and 70 meet and thus close the switch 26. The secondary circuit in the relay through the coil 22 is complete and the coil 22 in FIG. 1 is energized as soon as the ignition switch 12 is closed.

To prevent the electrical interlock from being permanently defeated by jamming the manually actuated plunger 90 in the depressed position illustrated in FIG. 4, the lower edge 104 of the plunger 90 contacts the clapper arm 50 and presses the clapper arm against the base plate 30 when the tang 82 is disengaged from the flexible conductor 60. The load contacts 52 and 54 of the switch 24 are, therefore, positively spaced from one another and the interlock relay 20 of FIG. 1 is not bypassed. It will be understood that if the plunger 90 in the depressed position did not hold the load switch 24 open, the switch 26 in the secondary circuit would always remain closed and the coil 22 could be energized every time the ignition switch was turned on to pull the load switch 24 closed. The extended lower edge 104 of the plunger 90, therefore, provided trip-free operation which means that the load contacts do not close until manual actuation to set the relay is fully completed.

FIG. 5 illustrates the relay 10 after manual actuation is fully completed. The plunger 90 has been returned to an elevated position by the return spring 96 in FIG. 2 so that the lower edge 104 is well above the clapper arm 50. With the plunger 90 elevated, the camming surfaces 100 and 102 are no longer engaged and the flexible latch 80 is returned to its unflexed position. When the ignition switch is turned on to energize the coil 22, the clapper arm 50 is pulled upwardly and brings the contacts 52 and 54 of the load switch 24 together. At this point, the interlock relay 20 in FIG. 1 has been by-passed and starting of the automobile engine is possible.

It will be observed in FIG. 5 that the lifting of the clapper arm 50 concomitantly lifts the flexible conductors 60 and 62 so that the conductor 60 slides over the inclined tang 82 to a position immediately above the tang. Lifting of the conductors comes about due to the engagement of the insulating pad 72 on the clapper arm 50 with the conductor 62 and the engagement of the contact 70 on the conductor 62 with the contact 68 on the conductor 60. The tang 82 does not interfere with the lifting of the conductor 60 since the latch 80 merely flexes laterally away from the conductor as the conductor engages the inclined lower surface of the tang during the upward movement.

When the ignition switch 12 in FIG. 1 is subsequently opened to shut the automobile engine off, the coil 22 of the relay is de-energized and the clapper arm 50 drops to its rest position illustrated in FIG. 3. The contacts 52 and 54 of the load switch 24 thus open and enable the interlock relay 20 in FIG. 1 to again perform

its intended function. In addition, the flexible conductor 62 assumes a rest position illustrated in FIG. 3 between the clapper arm 50 and the conductor 60. The conductor 60 having been located above the tang 82 in FIG. 5 and without the support provided by the clapper arm 50 and conductor 62, drops downwardly onto the tang as shown in FIG. 3. At the same time, contacts 68 and 70 of the switch 26 open and break the secondary circuit through the coil 22. The components of the relay have, therefore, all returned to their initial positions in which the relay is disabled and the electrical interlock relay 20 is again enabled. Subsequent override operations may be repeated as described above; however, each operation must be prefaced by manually actuating the plunger 90 since the relay automatically resets itself in a disabled condition whenever the ignition switch 12 is turned off.

While the present invention has been described in a preferred embodiment, it should be understood that modifications and substitutions in the detailed structure can be had without departing from the spirit of the invention. For example, the manually actuated plunger 90 and the latch 80 may take forms different from those illustrated provided that the camming surfaces of the latch and plunger engage one another while the plunger is depressed to deflect the latch and release the conductor 60 from its latched position on top of the tang 82. The flexible conductor 62 may rest on the insulating pad 72 at all times as suggested above. The coil 22 may be supported in an upright position relative to the clapper arm 50 as shown, for example, in copending application entitled Manually Set Magnetic Relay referenced above. Accordingly, the present invention has been described in a preferred embodiment by way of illustration rather than limitation.

#### I claim:

1. A manually set magnetic relay for one-time operations comprising:  
 first switch means operatively connectible in a load circuit and including a cantilevered, flexible clapper arm;  
 electromotive force generating means including a coil operatively connected with the clapper arm of the first switch means for closing the first switch means upon energization of the coil;  
 second switch means serially coupled with the coil to permit energization of the coil, the second switching means including first and second conductors having portions positioned in overlying relationship for flexing in and out of contact with thereby close and open the second switch means, the second conductor extending in transverse relationship to the clapper arm of the first switch means and being engaged by the clapper arm for flexing in and out of

contact with the first conductor of the second switch means;

latch means operatively engageable with the first conductor of the second switch means for holding the first conductor in a latched position out of contact with the second conductor of the second switch means;

the electromotive force generating means being operatively coupled to the first conductor of the second switch means for moving the first conductor into the latched position; and

manually operable actuator means engageable with the latching means for releasing the first conductor of the second switch means from the latched position.

2. A manually set magnetic relay as defined in claim 1 wherein:

the latch means includes a flexible latch mounted adjacent the first conductor of the second switch means for engagement with the first conductor and flexibly movable out of engagement with the first conductor.

3. A manually set magnetic relay as defined in claim 2 wherein:

the manually operable actuator means comprises a plunger mounted adjacent the latch for movement toward and away from the latch and disposed to flex the latch out of contact with the first conductor.

4. A manually set magnetic relay as defined in claim 3 wherein:

the plunger is a reciprocating plunger having a given axis of reciprocation; and

the latch includes of camming surface engaged by the plunger and disposed at an angle to the axis of reciprocation.

5. A manually set magnetic relay as in claim 1 wherein:

the first and second conductors of the second switch means are resiliently flexible conductors mounted in cantilever fashion with the free end portions of the conductors overlying one another for flexing in and out of contact; and

the latch means includes a resiliently flexible, one-piece latch having a tang engageable with the first conductor.

6. A manually set relay as defined in claim 5 wherein: the electromagnetic force generating means is operatively coupled to the first conductor of the second switch means by means of the clapper arm and the second conductor of the second switch means is engaged by the clapper arm.

\* \* \* \* \*

[54] TIME-DELAY CURRENT SENSING CIRCUIT  
BREAKER RELAY

[75] Inventor: James E. Hansen, Oak Creek, Wis.  
[73] Assignee: Eaton Corporation, Cleveland, Ohio  
[21] Appl. No.: 350,790  
[22] Filed: Feb. 22, 1982

Related U.S. Application Data

[63] Continuation of Ser. No. 119,055, Feb. 6, 1980, abandoned.  
[51] Int. Cl.<sup>3</sup> ..... H02H 3/08; H02H 3/093  
[52] U.S. Cl. .... 361/94; 361/92;  
361/104; 361/31; 335/152  
[58] Field of Search ..... 361/93-96,  
361/31, 104, 92, 97, 28, 195-198; 335/152, 154,  
301; 307/141, 293

[56] References Cited

U.S. PATENT DOCUMENTS

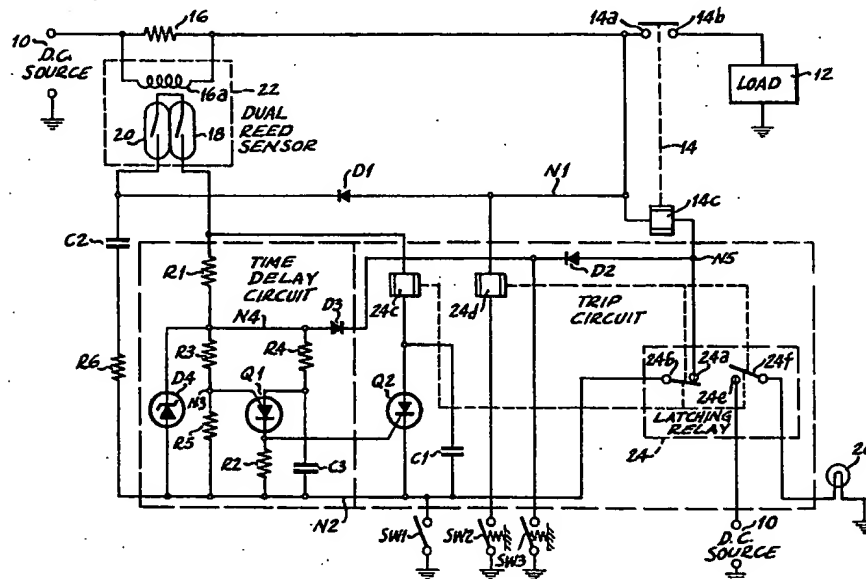
3,289,128	11/1966	Else	335/152
3,294,987	12/1966	Skrbina	361/93 X
3,309,571	3/1967	Gilker	361/94 X
3,434,080	3/1969	Mengelberg	335/154
3,471,813	10/1969	Neuber	335/152
3,538,386	11/1970	Schweitzer, Jr.	361/93 X
3,814,948	6/1974	Schuchmann et al.	307/141
3,970,908	7/1976	Hansen	318/221 E
4,006,443	2/1977	Kouchich et al.	361/104 X
4,103,317	7/1978	Krick	361/31
4,214,288	7/1980	Cavil et al.	361/92 X

Primary Examiner—Patrick R. Salce  
Attorney, Agent, or Firm—C. H. Grace; W. A. Autio

[57] ABSTRACT

A circuit control device combining the functions of a current sensor, a time delay circuit, an undervoltage sensor, and a lockout such that, once tripped, the device must be reset intentionally. The current sensor includes a coil (16a) surrounding two reed switches (18, 20), the reed elements (18a, 20a) of each of which being perpendicular to those of the other for vibration resistance. The coil is then surrounded by a magnetic shield (28) in order to shield out some of the leakage flux from the main relay coil (14c). The time delay circuit includes a PUT (Q1) which compares a steady voltage from a voltage divider network with the increasing voltage across a capacitor (C3). The undervoltage sensor includes a second PUT (Q3) which compares the voltage of the DC source (10) with the steady voltage across a zener diode (D5). In each case the cathode of the PUT is connected to the gate of an SCR (Q2) which, when gated "ON," energizes the trip coil (24c) of the latching relay (24), which in turn opens the main relay (14). This also closes another set of contacts (24e, 24f) in the latching relay, which activates a visual "tripped" indicator. The device also includes a reset coil (24d) to reclose the latching relay, an override switch (SW3) to energize the main relay coil regardless of the status of the latching relay, and an energy-storing capacitor (C2) to power the time delay circuit even when the DC source voltage drops too low to do so.

15 Claims, 4 Drawing Figures





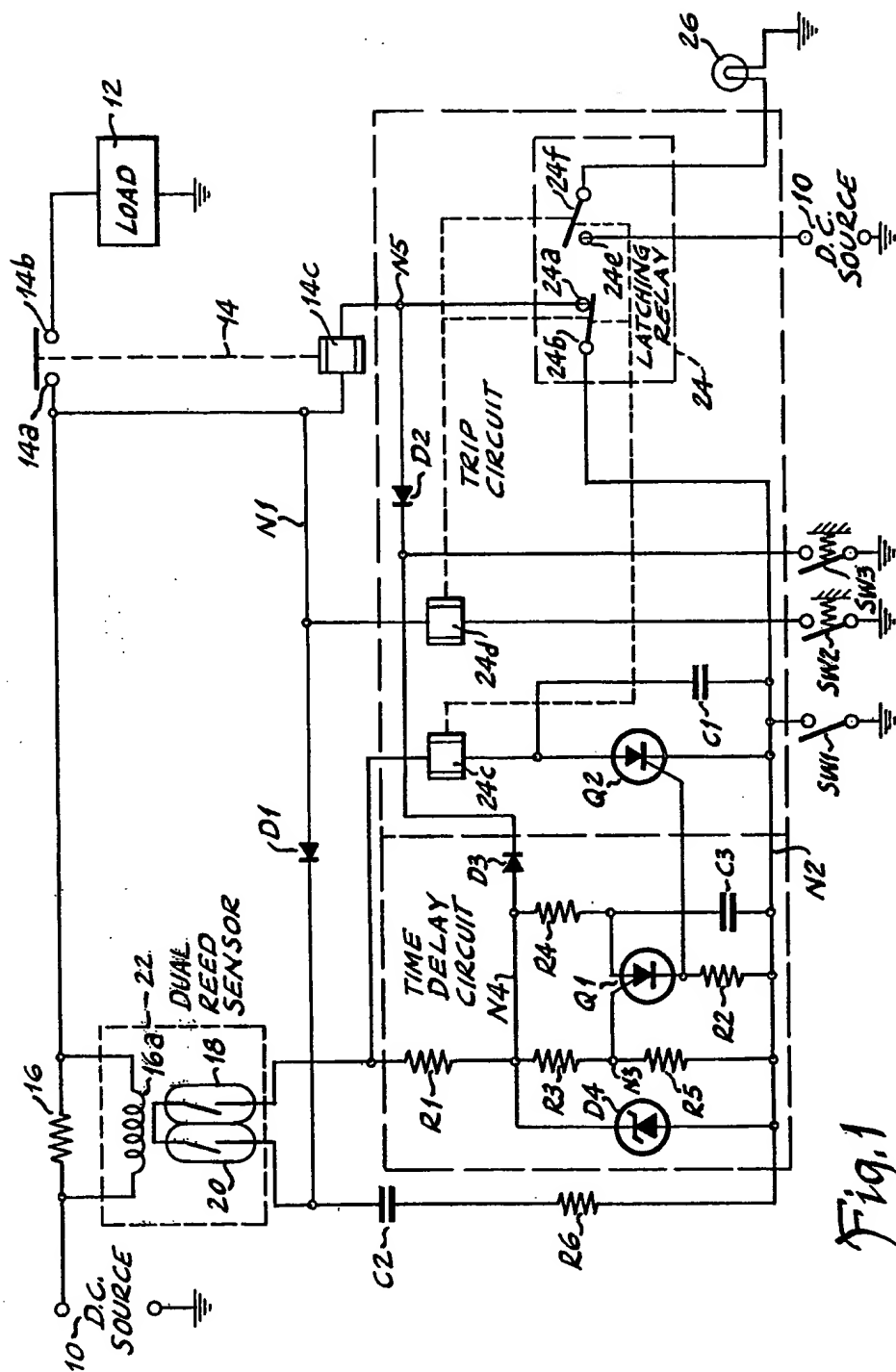


Fig. 1

Fig. 2

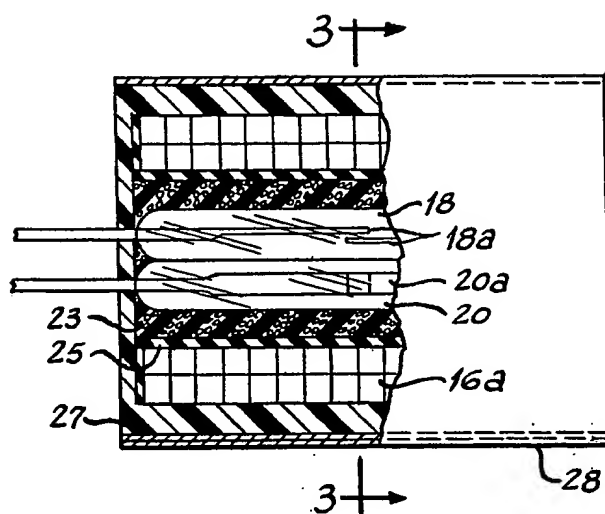
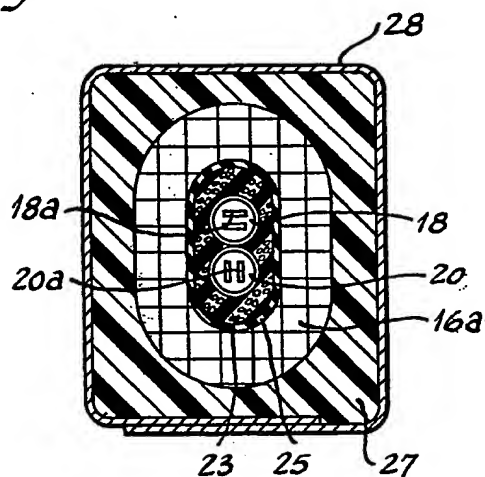
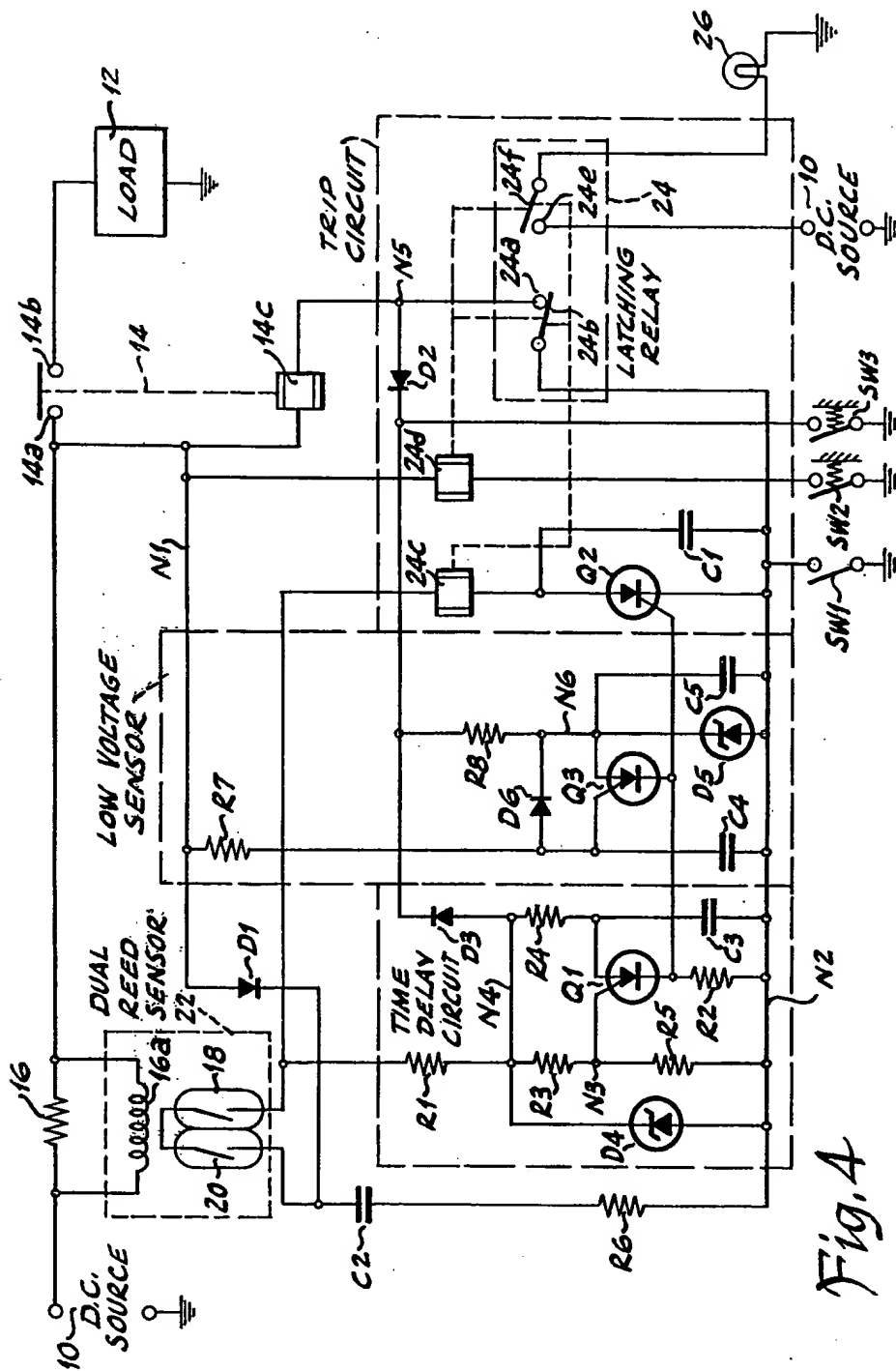


Fig. 3





## TIME-DELAY CURRENT SENSING CIRCUIT BREAKER RELAY

This is a continuation of James E. Hansen copending application Ser. No. 119,055, filed Feb. 6, 1980, now abandoned.

### BACKGROUND OF THE INVENTION

This invention pertains generally to relays which also perform circuit protective functions, such as those used as battery-to-electrical-system contactors in aircraft applications, and in particular to circuit breaker relays which trip open due to an overcurrent condition only after a predetermined period of time-delay.

There have been many circuits designed to be protective from certain conditions after a time delay. One example of such a circuit is Nurnberg et al U.S. Pat. No. 4,042,964, issued Aug. 16, 1977. The circuit there described, however, as well as others, did not provide all of the functions of an overcurrent sensor, a time delay circuit and an undervoltage sensor which control a latching relay which in turn controls a main relay.

Hansen et al U.S. Pat. No. 3,970,908, issued July 20, 1976, discloses the use of a reed switch to perform the function of a current sensor. This design, however, is subject to false indication of overcurrent due to vibration, and is thus unsuited to many applications.

An arrangement of several reed switches oriented at right angles to each other is disclosed in Neuber U.S. Pat. No. 3,471,813, issued Oct. 6, 1969. No means is there disclosed, however, to construct a vibration-resistant current sensor from those reed switches.

### SUMMARY OF THE INVENTION

The invention includes a dual reed current sensor, a time delay circuit, a latching relay which can be tripped and reset, and a main relay controlled by the latching relay. An alternative embodiment also includes an undervoltage sensor for opening the main relay if the battery voltage falls below acceptable levels. The current sensor includes two reed switches within the same coil which are connected in series. The two reed switches are mounted such that the reeds of one are perpendicular to those of the other, to provide greater resistance to false trips due to vibration.

An object of the invention is to provide a time delay circuit breaker relay.

Another object of the invention is to provide a relay as described above wherein threshold overcurrent conditions are sensed bilaterally by a dual reed current sensor.

Another object of the invention is to provide a relay as described above including a sensor which opens the relay when the voltage in the system drops below a predetermined level.

A more specific object of the invention is to provide a relay as described above which is resistant to vibration due to orthogonal mounting of the reeds of the dual reed current sensor, and due to solid state construction of logic functions.

Another specific object of the invention is to provide a relay as described above which has a differential between the level of trip current in one direction and that in the other direction.

Another specific object of the invention is to provide a relay as described above wherein the time delay and

undervoltage sensing are provided by electronic circuits.

Other features of this invention include an override function for intentionally inhibiting the current sensor function when high currents are anticipated for periods exceeding the internal delay period; a lockout function once the main relay is tripped; a reset function; and provision for indication of "tripped" condition.

Other objects and advantages will hereinafter appear.

### DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagrammatic view of a circuit constructed according to the invention.

FIG. 2 is a side view of the reed switches, coil, and magnetic shield, with the coil and magnetic shield partially cut away.

FIG. 3 is a cross-sectional view of FIG. 2 taken along line 3-3.

FIG. 4 is a diagrammatic view of a circuit constructed according to an alternate form of the invention.

### DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to FIG. 1, the circuit embodying this invention includes a D.C. source 10 connected in series with a load 12 through the contacts 14a and 14b of a main relay 14. In the line between source 10 and the main relay contacts is a tapped shunt 16. Connected in parallel with shunt 16 is a coil 16a for sampling the current passing through the line at that point at any one time. The respective currents through the shunt 16 and coil 16a are in inverse proportion to their respective resistances. Thus the amount of current passing through the coil 16a can be increased by increasing the resistance of the shunt or decreasing the resistance of the coil. And this ratio of currents can be preserved over a wide range of temperature by constructing both the shunt and the coil of the same metal.

Coil 16a has an air core, in which are inserted two reed switches 18 and 20. These two reed switches are connected in series. Their long axes are arranged in parallel relation, side by side, as shown in FIG. 2, with the reed elements of one rotated 90 degrees with respect to those of the other, so that the reed elements 18a and 20a of the two switches are perpendicular to each other, as shown in FIG. 3. Thus vibration in any one plane will not be orthogonal to both reed switches. Hence, with the two reed switches connected in series, the combination is much more resistant to false trip due to vibration or shock impulse than would a single reed switch be.

The shunt 16, coil 16a and reed switches 18 and 20 make up the dual reed current sensor 22.

As illustrated in FIGS. 2 and 3, immediately surrounding the two reed switches is a layer of soft, spongy material 23 to insulate the switches from mechanical shock and vibration. This layer is surrounded by a bobbin 25 upon which coil 16a is wound. A layer of epoxy 27 is then applied to the coil, and the entire assembly is inserted into a magnetic shield 28.

One of the reed switches 20 of the current sensor 22 is connected through a diode D1 to the node N1 between the unswitched side 14a of the main relay contacts and shunt 16. Diode D1 is oriented to allow current to flow to the reed sensor, not away from it. The same reed switch 20 is connected to ground through a capacitor C2, a resistor R6 and a switch SW1. Node N2 is the node between resistor R6 and switch SW1.

Reed switch 18 is connected to node N2 through the time delay circuit, which includes a voltage divider made up of three resistors R1, R3 and R5. Zener diode D4 is connected in parallel with resistors R3 and R5 to regulate the voltage thereacross. Connected to the node N3 between resistors R3 and R5 is the gate of a programmable unijunction transistor (PUT) Q1. The anode of Q1 is connected to the node N4 between resistors R1 and R3 through a resistor R4, and to node N2 through a capacitor C3. The cathode of Q1 is connected to node N2 through a resistor R2, and is connected directly to the gate of a semiconductor-controlled rectifier (SCR) Q2. The cathode of SCR Q2 is connected to node N2.

One end of the coil 14c of the main relay 14 is connected to node N1, while the opposite end of coil 14c, as shown in FIG. 1, is connected to a contact 24a of latching relay 24. The opposite contact 24b of relay 24 is then connected to node N2. Since relay 24 is a latching relay, separate coils are needed to open and close it. Trip coil 24c of relay 24, which opens these contacts when energized, is connected between reed switch 18 and the anode of SCR Q2. A capacitor C1 is connected between the anode and cathode of SCR Q2 to prevent voltage transients from accidentally forcing Q2 into conduction. Set coil 24d, which closes contacts 24a and 24b when energized, is connected between node N1 and a momentary switch SW2, which connects the set coil circuit to ground when closed.

The operation of this circuit breaker relay can be described as follows: Assuming latching relay 24 is closed, closing the switch SW1 closes the main relay 14, and opening the switch opens the relay. Closing switch SW1 also causes capacitor C2 to charge. The purpose of capacitor C2 is to provide current to the time delay circuit and trip circuit in case the voltage level of the DC supply 10 falls too low to do so due to an overload. Resistor R6 is a low level resistance put into the circuit to fuse open should capacitor C2 short out, so that C2 would then be removed from the circuit.

On the occurrence of a predetermined overload level of current, the dual reed current sensor closes due to the force created in the coil surrounding the reed switches. This energizes the time delay circuit such that the voltage at the gate of PUT Q1 is set at the voltage across resistor R5 whereas the voltage across capacitor C3, which is the anode voltage of PUT Q1, begins to increase. The time required for the voltage across capacitor C3 to reach the voltage across R5 is determined by the values of R3, R4, R5 and C3. When that voltage is reached, PUT Q1 sends a pulse of current to the gate of SCR Q2 which, in turn, energizes the trip coil 24c of the latching relay 24, opening relay 24, which finally opens main relay 14 by de-energizing its coil 14c.

In addition, latching relay 24 has another set of contacts 24e and 24f, which are always open when contacts 24a and 24b are closed, and vice versa. One of these contacts 24e and 24f is connected to DC source 10, while the other is connected through a lamp 26 to ground the function of which is to indicate a tripped condition when contacts 24a and 24b open, since contacts 24e and 24f would then be closed.

Another momentary switch SW3 is connected through a diode D2 to the node N5 between the main relay coil 14c and latching relay contact 24a, and through another diode D3 to node N4 to shunt the time delay circuit to ground and reset the same. Switch SW3 is an "override" switch. When this switch is closed, the main relay coil 14c is directly energized, and the main

relay 14 is closed, regardless of the condition of the rest of the circuit. Thus it is possible, by using this switch, to inhibit the current sensor and trip function on certain occasions when high currents are anticipated for periods exceeding the period of the time delay circuit, such as during start-up of certain types of loads. Since the main relay is energized directly, it can be energized even if the device has been tripped and not subsequently reset.

An additional feature of this current sensor is that it is bidirectional, that is, the reed switches 18 and 20 close at the same current level regardless of the current polarity. If a differential between the trip current in one direction and that in the other is desirable, however, this can be accomplished by use of an additional unidirectional source of magnetic flux, positioned near the reed switches. This source of flux could be a permanent magnet, a separate coil added for that purpose, or preferably the main relay coil, which creates sufficient additional unidirectional leakage flux to result in a sufficient differential. The actual amount of the differential can be controlled by the shape and thickness of the shield 28 shown in FIGS. 2 and 3.

An alternate embodiment of the invention is shown in FIG. 4. The circuit there illustrated is similar to that shown in FIG. 1, except that a low voltage sensor has been added to open the main relay 14 in the event that a massive overload draws the voltage of the DC source 10 below the relay's hold-in voltage before the time delay circuit opens the relay.

This low voltage sensor circuit includes a resistor R7 connected to node N1, and connected through a capacitor C4 to node N2. Connected to the junction between resistor R7 and capacitor C4 are the anode of a diode D6 and the gate of a second PUT Q3. The cathode of PUT Q3 is connected in parallel with the cathode of PUT Q1 to the gate of SCR Q2. The cathode of diode D6 is connected to the anode of PUT Q3 to form a node N6. The cathode of a diode D5 is connected to node N6, while the anode is connected to node N2. A capacitor C5 is connected in parallel with diode D5. Finally, a resistor R8 is connected between node N6 and override switch SW3.

In operation, the voltage of the DC source 10 appears across capacitor C4, that is, between the gate of PUT Q3 and node N2. Meanwhile, a constant voltage, less than the DC source voltage, regulated by zener diode D5, appears between the anode of PUT Q3 and node N2. When the DC source voltage drops to less than the voltage across zener diode D5, as could happen during a severe fault, PUT Q3 becomes conductive, allowing capacitor C5 to force a pulse of current into the gate of SCR Q2, making it conductive. This energizes the trip coil 24c, opening the main relay 14 as previously described.

It should be recognized and understood that various modifications of the invention herein described are possible without departing from the scope of the appended claims.

What is claimed is:

1. A circuit breaker relay, comprising:
  - an electrical DC battery power supply source;
  - a load circuit including power switching means controllable to connect said source to a load;
  - a pilot switch operable to control said power switching means for energization and deenergization of said load;

current sensing means, comprising normally open reed relay contact means operable to close for indicating that the current flowing in said load circuit has reached a predetermined level; and circuit control means connected through said reed relay contact means to the power supply source side of said power switching means for opening said power switching means in response to said indication from said current sensing means that said current has reached said predetermined level;

said circuit control means comprising a time delay circuit and a trip circuit normally without supply power, said time delay circuit responding to closure of said contact means for precisely providing a predetermined time delay and then signaling said trip circuit, which in turn deenergizes said power switching means, disconnecting said load from said source;

and energy storage means connected to the power supply source side of said power switching means for supplying operating voltage through said reed relay contact means to said time delay circuit and said trip circuit in the event the voltage of said DC battery source should drop low on a high overload.

2. A circuit breaker relay as recited in claim 1, further comprising low voltage trip means for sensing the voltage of said source and signaling said trip circuit to deenergize said power switching means when the voltage of said source falls below a predetermined low level, regardless of the indication of said current sensing means and the signal of said time delay circuit.

3. A circuit breaker relay as recited in claim 2 wherein said trip circuit comprises:

- visual indication means for indicating that said power switching means has been deenergized by said trip circuit;
- a latching relay having two sets of contacts arranged such that whenever one set of contacts is closed, the other set is open, the first set of contacts being connected to energize said power switching means, and the second set of contacts being connected to energize said visual indication means;
- trip control semiconductor switching means having anode, cathode and gate terminals;
- a trip coil connected in series with said semiconductor switching means such that on receipt by said semiconductor switching means of said signal from said time delay circuit or said low voltage trip means, said trip coil is energized, opening said first set of contacts and closing said second set of contacts;
- manual switching means;
- a reset coil connected in series with said manual switching means, such that when said manual switching means is closed, said reset coil is energized, closing said first set of contacts and opening said second set of contacts.

4. A circuit breaker relay as recited in claim 3 further comprising a coil on said power switching means, and an override circuit including an override switch connected to said coil of said power switching means, such that when said override switch is closed, said coil is energized regardless of the condition of said first set of contacts of said latching relay.

5. A circuit breaker relay as recited in claim 3 wherein said time delay circuit comprises:

- time delay semiconductor switching means having a gate terminal, an anode terminal and a cathode

- terminal, said cathode terminal being connected to the gate terminal of said trip control semiconductor switching means of said trip circuit;
- voltage divider means for supplying a constant voltage to said gate terminal of said time delay semiconductor switching means;
- and resistance-capacitance means connected to said anode terminal of said time delay semiconductor switching means such that when the voltage across said capacitance reaches the voltage supplied to said gate terminal thereof, a pulse of current is sent from said cathode terminal thereof to said trip control semiconductor switching means of said trip circuit, said pulse of current constituting said signal from said time delay circuit to said trip circuit.

6. A circuit breaker relay as recited in claim 5 wherein said low voltage trip means comprises:

- low voltage control semiconductor switching means having a gate terminal, an anode terminal and a cathode terminal, said cathode terminal thereof being connected to the gate terminal of said trip control semiconductor switching means of said trip circuit; and
- a zener diode for supplying a constant voltage to said anode terminal of said low voltage control semiconductor switching means;
- said DC battery power supply source being connected to said gate terminal of said low voltage semiconductor switching means such that when the voltage supplied to said gate terminal thereof by said source drops below that supplied to said anode thereof, a pulse of current is sent from said cathode terminal thereof to said trip control semiconductor switching means of said trip circuit, said pulse of current constituting said signal from said voltage trip means to said trip circuit.

7. A circuit breaker relay as recited in claim 1, further comprising unidirectional conducting means connected between said energy storage means and said DC battery source for preventing return of the energy from said energy storage means to said source.

8. A circuit breaker relay as recited in claim 1 further comprising an impedance in series with said energy storage means for fusing open in the event that said energy storage means shorts, such that said energy storage means is removed from the circuit.

9. A circuit breaker relay as recited in claim 1 wherein said current sensing means comprises a reed relay having a coil for sensing the current in said load circuit and said normally open contact means serving as a switching means.

10. A circuit breaker relay as recited in claim 9 wherein said normally open contact means comprises a pair of reed switches connected in series and having reed elements, the reed elements of one of said reed switches being arranged in perpendicular relation with respect to the reed elements of the other of said reed switches, such that said normally open contact means is more resistant to closure due to vibration than a single reed switch or a plurality of reed switches having parallel elements.

11. A circuit breaker relay as recited in claim 10 wherein said current sensing means comprises:

- a source of unidirectional magnetic flux providing a differential between the trip currents in opposite directions in said load circuit;

wherein said reed switches are physically located sufficiently close to said source of unidirectional flux that its operation is affected by said flux; and magnetic shielding means between said source of unidirectional flux and said reed relay for controlling the degree that said reed switches are affected by said flux.

12. A circuit breaker relay as recited in claim 11 wherein said source of unidirectional flux comprises a coil connected across said DC source for providing said flux.

13. A circuit breaker relay as recited in claim 11 wherein said power switching means is a relay having normally open switching means and a coil which produces flux including leakage flux, said coil being said source of unidirectional magnetic flux.

14. A circuit breaker relay as recited in claim 7 wherein said source of unidirectional flux comprises a permanent magnet for providing said flux.

15. A circuit breaker relay comprising:  
an electrical DC power supply source;  
a load circuit including power switching means controllable to connect said source to a load;  
a pilot switch operable to control said power switching means for energization and deenergization of said load;

current sensing means for indicating that the current flowing in said load circuit has reached a predetermined overload level;

said current sensing means comprising a reed relay having a coil connected to the power supply source side of said power switching means for sensing the overload current in said load circuit and a pair of reed switches connected in series and having the plane of closure motion of the reed elements of one of said reed switches arranged at a right angle relative to the plane of closure motion of the reed elements of the other reed switch so as to be effectively shock and vibration resistant;

circuit control means connected to the power supply source side of said power switching means for opening the latter on said indication from said reed relay that said current has reached said predetermined overload level;

and said circuit control means comprising a time delay circuit and a trip circuit, said time delay circuit comprising means for precisely providing a predetermined time delay and then signaling said trip circuit which thereupon deenergizes said power switching means whereby to disconnect said load from said source.

30

35

40

45

50

55

60

65



US005313189A

**United States Patent** [19]

Dodd et al.

[11] Patent Number: **5,313,189**[45] Date of Patent: **May 17, 1994**

[54] **VEHICLE WHEEL SAFETY BARRIER SYSTEM USING PRESSURE AND INFRARED SENSORS**

[75] Inventors: Ian Dodd, Rigaud; James Anglehart, Montreal, both of Canada

[73] Assignee: BBI Fibre Technologies, Inc., Quebec, Canada

[21] Appl. No.: 954,529

[22] Filed: Sep. 30, 1992

[51] Int. Cl.<sup>5</sup> ..... B60Q 1/26

[52] U.S. Cl. .... 340/433; 340/903; 340/905

[58] Field of Search ..... 340/433, 903, 904, 942, 340/905, 521; 180/281

[56] References Cited

**U.S. PATENT DOCUMENTS**

4,260,980	4/1981	Bates	340/904
4,300,116	11/1981	Stahovec	340/904
4,518,183	5/1985	Lee	293/118
4,688,656	8/1987	Kent	180/279
4,688,824	8/1987	Herring	280/762
4,694,295	9/1987	Miller	340/903
4,763,939	8/1988	Zhu	293/17
4,877,266	10/1989	Lamparter et al.	280/762

4,956,630	9/1990	Wicker	340/433
4,983,949	1/1991	Wicker	340/433
5,042,858	8/1991	Schubert et al.	293/24

**FOREIGN PATENT DOCUMENTS**

809624 2/1959 United Kingdom

*Primary Examiner*—Hezron E. Williams

*Assistant Examiner*—Christine K. Oda

*Attorney, Agent, or Firm*—Merchant, Gould, Smith, Edell, Welter & Schmidt

[57] **ABSTRACT**

The safety barrier system prevents a person from being caught under a wheel of a vehicle and is provided with a sensing system to inform the driver of the presence of the person on the barrier during start up. The sensing system combines a first sensor (for example, a pressure sensor) with an infrared sensor, and includes a snow switch for selectively using the first sensor and/or the infrared sensor depending on the weather conditions. The barrier is mounted to the vehicle by a motor drive mechanism to lower the barrier when stopped and to raise the barrier after the vehicle has travelled a given distance. The system is particularly suitable for school buses.

10 Claims, 8 Drawing Sheets

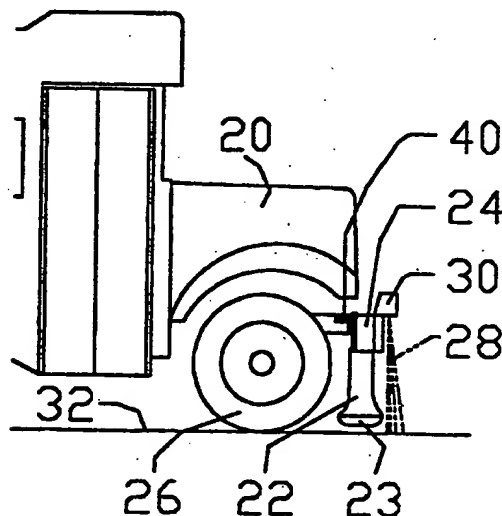




Fig. 1

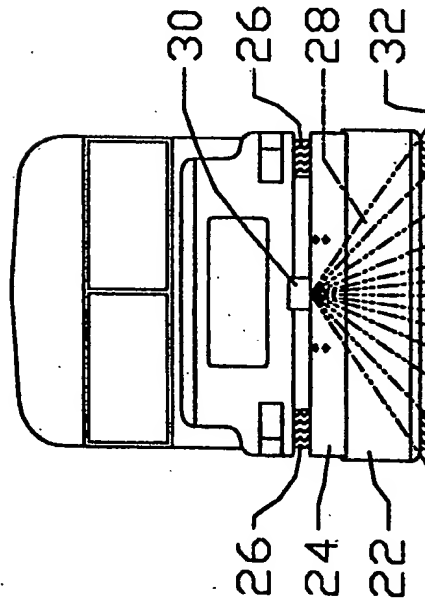


Fig. 2

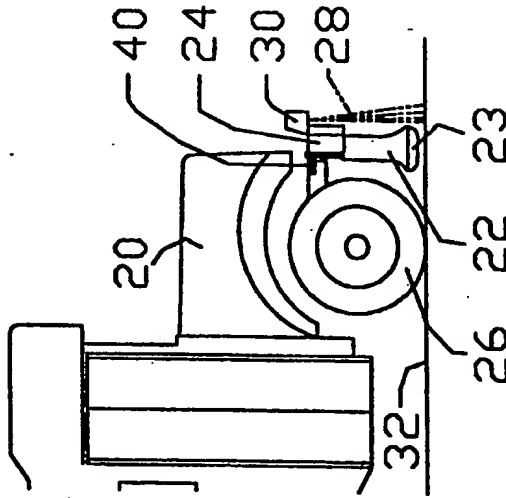


Fig. 3.

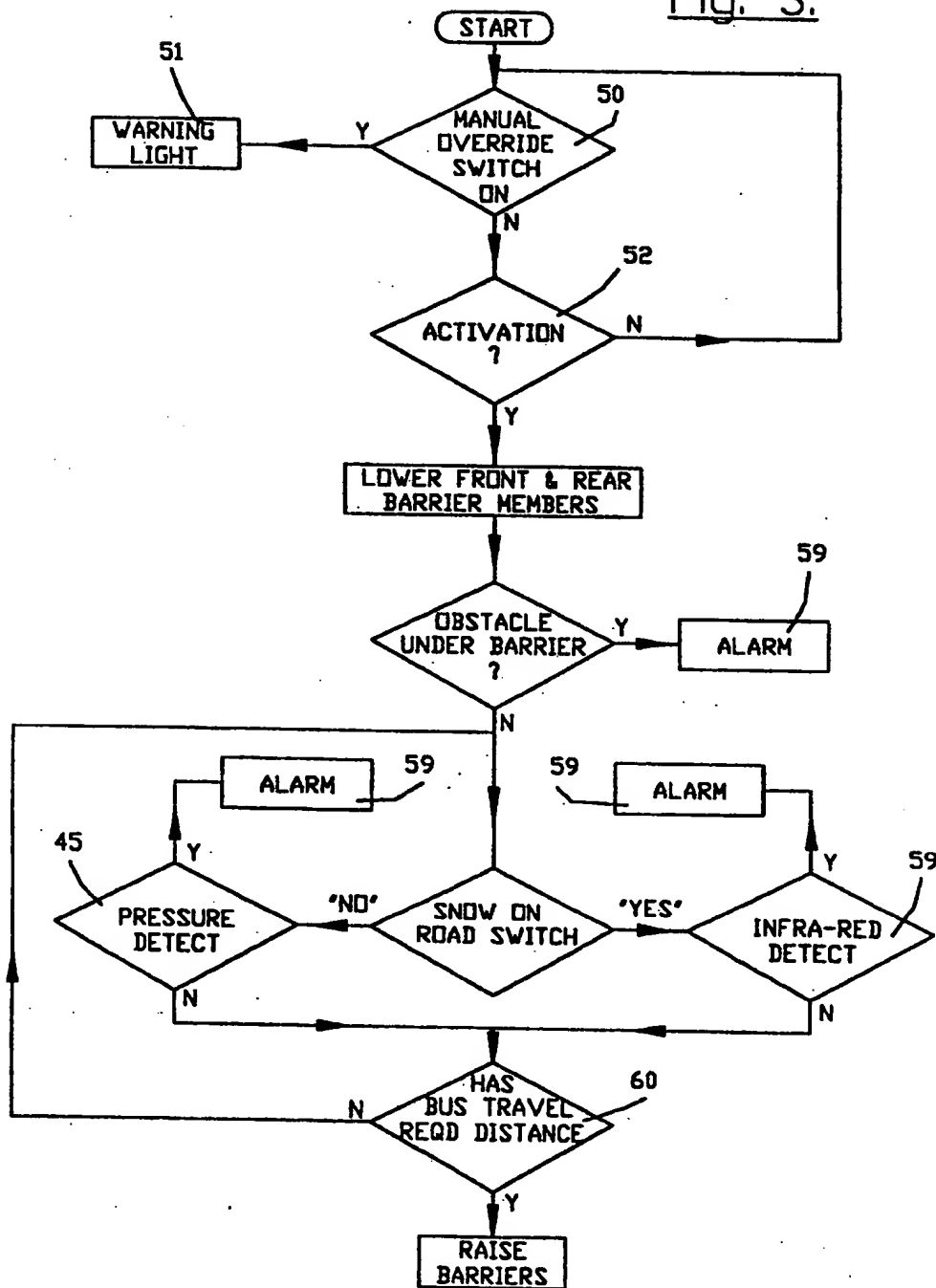


Fig. 4

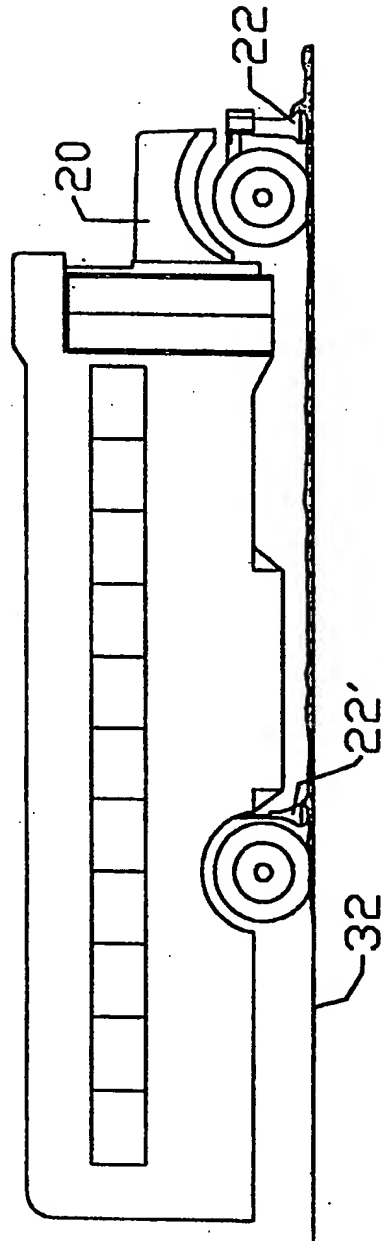


Fig. 5

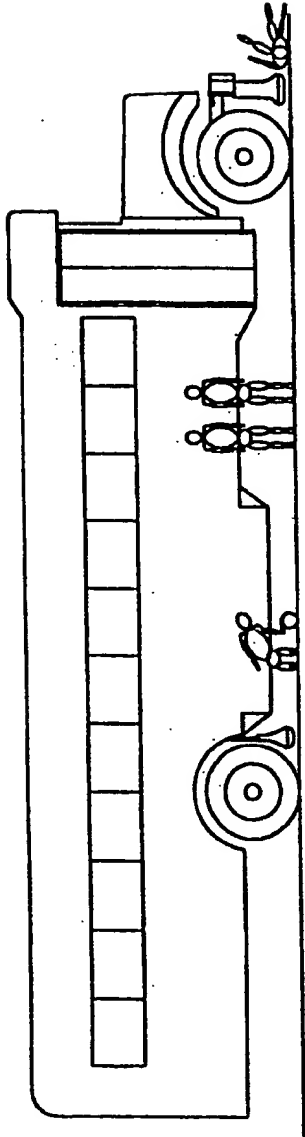


Fig. 6

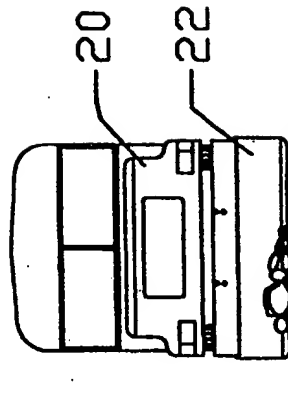


Fig. 8

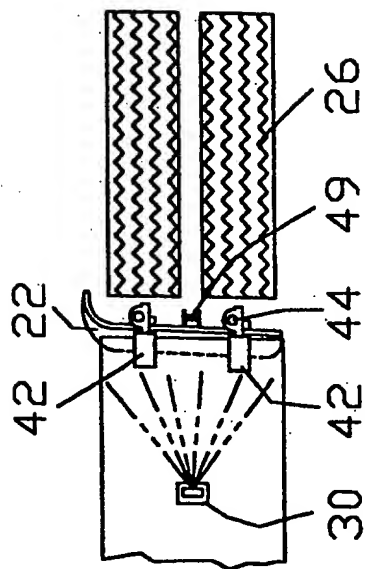


Fig. 7

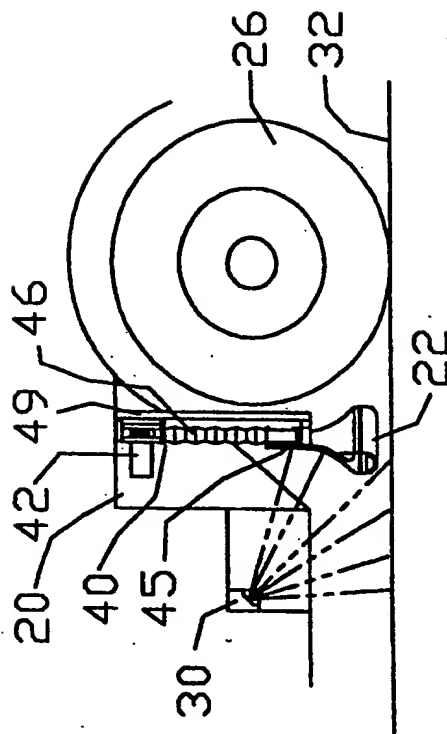


Fig. 9

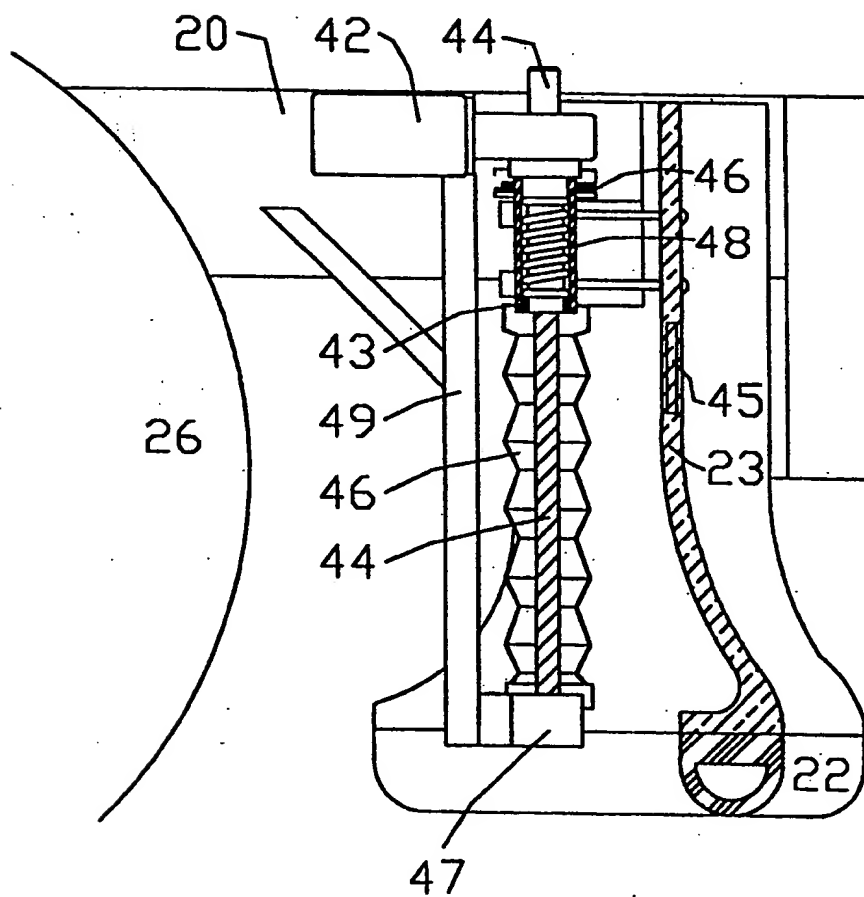


Fig. 10

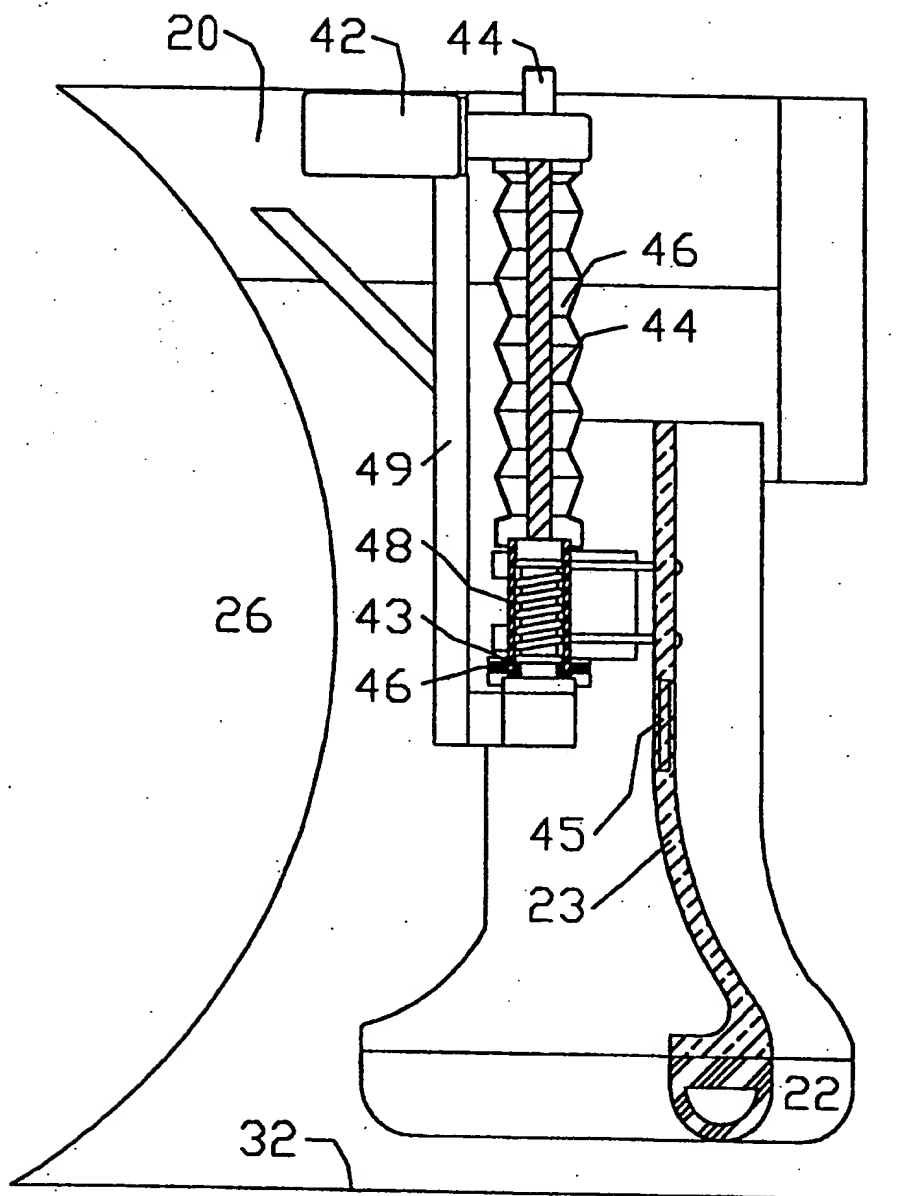
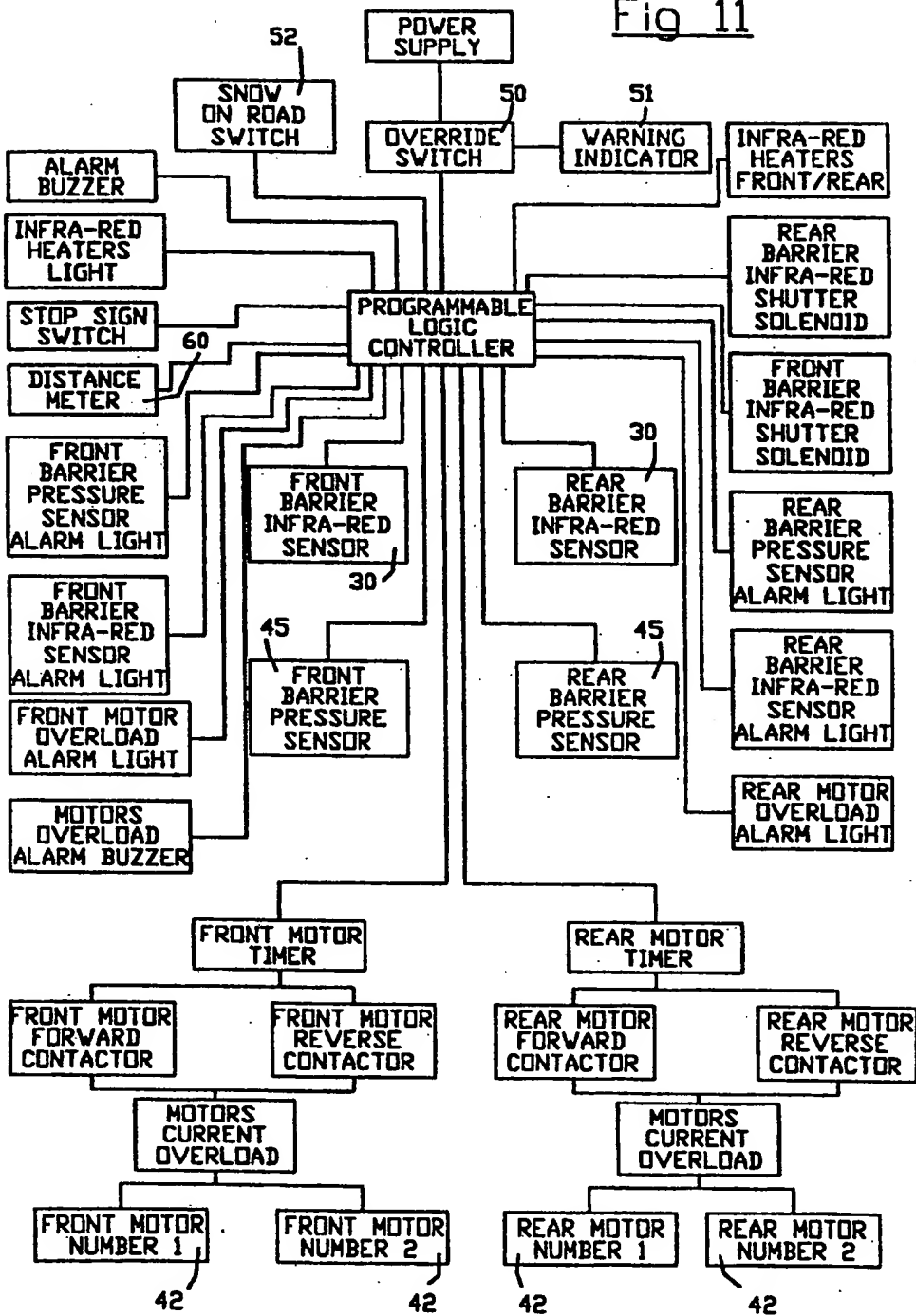


Fig 11





## VEHICLE WHEEL SAFETY BARRIER SYSTEM USING PRESSURE AND INFRARED SENSORS

### FIELD OF THE INVENTION

The present invention relates to a vehicle wheel barrier system for preventing people from being caught beneath a vehicle wheel and being injured as the vehicle starts up. In particular, the present invention may be applied to school buses to prevent children from being caught by the wheels as the school bus starts up after making a drop off.

### BACKGROUND OF THE INVENTION

It is a known problem with school buses that as children are let off after school at the various stops that the school bus makes on its route to drop off children, that bus driver supervision of the children surrounding the bus is particularly difficult to ensure that no children have slipped underneath the bus either accidentally or intentionally. This is particularly difficult since several children may be getting off the bus at the same time and to monitor the movements of all children getting off the bus is virtually impossible, and even with the best mirror systems, there is no guarantee that a child does not slip under the bus and out of the view of the mirror system.

As early as 1959 in British Patent Specification 809,624, it was known to provide safety devices fitting in front of wheels on buses and cars in order to provide a barrier preventing a pedestrian from being caught underneath the wheels of the vehicle. These devices were fixed in nature, and were not particularly practical. U.S. Pat. Nos. 4,688,824 and 4,877,266 are examples of more recent safety devices for school buses which serve to prevent children from being caught under the wheels which are of a more practical construction. U.S. Pat. No. 4,688,656 describes a barrier safety device in which contact with the device activates means for turning off the motor vehicle.

In the prior art systems, no effective combination of a safety barrier and a detecting means to indicate the presence of a person or an object in closed proximity or in contact with the safety barrier has been constructed. It is important for such safety barriers to completely eliminate the possibility that a child or object be caught under the wheels and also to prevent that the child be pushed or dragged.

### SUMMARY OF THE INVENTION

It is an object of the present invention to provide a vehicle wheel safety barrier system having a safety barrier and means to detect the presence of a person or child in contact with and/or in close proximity to the safety barrier in order to signal the driver to stop the vehicle. To achieve this object, in all climate conditions, it is an object to provide a vehicle wheel safety barrier system which is able to operate when the roads are clear and hot as well as when the roads are covered with snow. This object is achieved by combining an infrared sensing system able to detect a person's presence near the barrier when snow conditions are prevailing with another sensing system which is able to detect the presence of an object near the barrier more effectively under clear or warm conditions.

It is important to consider that most sensing systems would detect the build up of snow on the safety barrier as contact with the barrier or movement in front of the

barrier, since the snow would be detected as an object by the sensing system. For example, ultrasonic or microwave detectors detect snow much as they detect people. Infrared detectors most commonly detect changes in a total amount of infrared radiation received from an optically divided viewing or detection zone. Thus, motion in the zone by an object emitting infrared radiation at a different level than that of the background will cause a change in the total amount of infrared radiation received, and in this way motion is detected.

Infrared sensing systems do not react to the motion of objects having the same infrared emitting characteristics as their background, and the infrared system of the present invention has a chosen sensitivity such that the accumulation of snow on the barrier is not detected as motion in front of the barrier. On the other hand, infrared detection can be easily influenced by temperature variations which are more likely when the ambient temperature is higher or more particularly when the insolation is greater. Thus it is possible to make use of infrared detection under snow conditions when it provides a reliable means of detection, and to make use of other more effective detection means, such as pressure, ultrasound, microwave, and light beam interrupt which measure physical presence of objects independently of the emission characteristics, under clear conditions when such detection means are unaffected by snow.

According to the invention there is provided a vehicle wheel safety barrier system comprising a barrier member for blocking an object from reaching at least one wheel of the vehicle as it is moving; motor mount means for raising and lowering the barrier member, and for connecting the barrier member to a frame of the vehicle; first sensing means for detecting when the object comes in contact with or near the barrier member and for producing an output signal; infrared sensing means for detecting infrared radiation in a zone in front of the barrier member and for producing an output signal; selecting means for providing a climate condition signal indicative of a weather condition outside the vehicle; and means to generate a warning alarm when the barrier member is lowered, as a function of the climate condition signal and the output signals of the first sensing means and the infrared sensing means. In this way, the generating means ignore the output signal of the infrared sensing means under weather conditions unsuitable for infrared radiation detection, and of the first sensing means under weather conditions unsuitable for detection using the first sensing means.

### BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be better understood by way of the following detailed description of a preferred embodiment with reference to the appended drawings in which:

FIG. 1 shows a front view of a school bus equipped with a safety barrier system according to the preferred embodiment;

FIG. 2 is a side view of a front portion of a school bus equipped with the safety barrier system according to the preferred embodiment;

FIG. 3 is a flow chart of the electronic control system according to the preferred embodiment;

FIG. 4 shows a full side view of a school bus equipped with the safety barrier system according to the preferred embodiment travelling on a road surface with snow thereon;

FIG. 5 shows a full side view of a school bus provided with the safety barrier system according to the preferred embodiment with children on the side and in front of the bus;

FIG. 6 is a front view of a child being pushed by the safety barrier system at a front of the bus;

FIG. 7 is a partially cross-section side view of the safety barrier system provided on the rear wheel set of a school bus;

FIG. 8 shows a plan view of the barrier safety system installed at the rear wheels of the bus;

FIG. 9 shows a partly cross-sectional view of the barrier motor mount system in the raised position;

FIG. 10 shows a view similar to FIG. 9 with the barrier lowered; and

FIG. 11 is a block diagram of the electromechanical system according to the preferred embodiment.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the preferred embodiment, the safety barrier system comprises a front vertically movable fiberglass barrier member (22) mounted to the front part of the frame of a school bus (20) (see FIGS. 1 and 2), as well as a rear barrier member (22') mounted to a rear wheel well of the bus (20). (see FIGS. 7 to 10) A flexible plastic or rubber skirt (23) is fitted to the bottom of barriers (22, 22'). At the front of the bus 20, the member 22 is mounted between front bumper 24 and the tires 26.

Motor mount means (40) each comprise a DC electric drive motor (42) for turning a threaded shaft (44) which a nut (43) turns, the nut (43) being connected to the barrier (22, 22'). Upper and lower gaiters (46) cover each upper and lower part of the shaft (44) to protect it from the elements. The nuts (43) are connected to the barriers (22, 22') by a spring mount (48) which allows a small amount of resilient ride up of barrier (22, 22') on the nuts (45) in case there is a small rock or clump of ice on the road surface (32). If the object under the barrier (22) or (22') is large enough to interfere with descent in spite of the spring mount (48), the motor (42) will 'overload', i.e. it will draw a large current, and as will be described below, the overload is to be detected and a warning alarm will sound. The motor (42) will then go into reverse and thus raises the barrier (22, 22').

The shaft (44) is mounted between motor (42) and a bearing (47) at the bottom of a C-shaped channel member (49) connected to bus (20). Pressure transducers (45) provided inside the barrier (22, 22') are used to generate an electrical signal when an object contacts the barrier. Transducers (45) are preferably passive transducers which convert the pressure or change in pressure on the barrier (22, 22') into an electrically measurable characteristic such as resistance, capacitance or voltage, as is known in the art.

The safety barrier system according to the invention uses an infrared detector means (30) to detect the presence of a person immediately in front of the barriers (22) and (22'). As shown, the infrared detector (30) observes infrared radiation in a 'curtain' 28 the full width of the barrier (22) or (22') and 'sees' only the barrier or object placed very near or on it.

With reference to FIG. 3, the operation of the preferred embodiment will now be described. When the bus is turned on, power is provided to the safety system's electronic controls. A manual override switch (50), which may be part of a keypad command entry system, is provided to allow the bus driver to turn the

system off, however, a warning light (51) will remain on while the system is off. Next, the 'snow on road switch' (52) is read to determine its state. Now, once the system is activated, either by manual activation, opening the bus door, stopping for a predetermined time period, or turning on the stop signals of the school bus, the system begins to lower the front and rear barrier members (22) and (22').

The motors (42) are turned on to lower the barriers (22) and (22') for a given time period. If a current overload is detected, it is assumed that there is an object under the barrier (22, 22') and the operator is given a warning alarm (57) to check the barrier. The barriers (22, 22') are then raised. Once the timer indicates that the barriers have fully descended, the system uses a distance meter (60) to determine if the bus (20) has travelled a required distance. The required distance may be as little as 6 meters, although 12 meters may be used. The distance meter may be part of the vehicle's odometer.

Until the bus (20) travels the required distance, the system selectively uses the first detecting means (45) (i.e. the pressure sensing means) or the infrared detector means (30) to determine if a person has made contact with the barrier (22, 22'), in which case alarm (59) is triggered. In the preferred embodiment, the system uses the infrared detection (30) when the snow switch is on and the pressure detection (45) whenever the switch (50) indicates there is no snow on the road (this is of course controlled by operator input). In this way, false alarms that would be generated by the pressure detection (45) when snow and ice on the road pushes against the barrier (22, 22') are eliminated. During snow conditions, the infrared detector (30) works effectively without false alarms being generated by snow being ploughed by the barrier (22, 22'). During hot temperatures, and during full insolation, the risk that pockets of warm air rising from the road surface (32) cause false alarms in the infrared detector (30) is eliminated by ignoring the infrared detector (30).

As shown in FIG. 4, when the road surface (32) is covered with snow the barrier members (22 and 22') will push or plow the snow when the barrier members are lowered and the bus begins to start up. As shown in FIG. 5, children surrounding the bus may be in danger if the child slips in front of the bus or underneath the bus at the side near the rear. Children standing upright at the side of the bus behind the exit doors or on the other side of the bus are in less danger due to the driver's ability to see the children using standard mirrors. As shown in FIG. 6, a child fallen in front of the bus would be pushed by barrier (22) as the bus starts up.

As shown in FIG. 11, the preferred electronic control system uses a programmable logic controller (PLC) for controlling the safety barrier system. The system is activated for example using the stop sign switch which will cause the programmable logic controller to carry out the sequence of steps shown in FIG. 3. In addition to the step shown in FIG. 3, other components are activated as will be described below. The programmable logic controller, and the entire system is shut down if the manual override switch (50) is switched on giving power only to the warning indicator (51). When the override switch is off control is given to the programmable logic controller. The state of the snow on road switch (52) is recorded by the programmable logic controller. When the state of the snow flag is set to YES, the system prepares the infrared detectors (30) by

turning on the infrared sensor heaters both at the front and the rear. An infrared heater's light is turned on to show that the heaters are working.

Whenever the stop sign switch is activated, the system signals the front and rear motor timers to activate the front and rear motor forward contactors to lower the front and rear barriers by activating both front and rear motors. If either the front or rear motors draw an excess current, motor current overload sensors provide a signal to the PLC which will signal the appropriate motor timer to reverse the motors until raised. If a current overload is detected, it is assumed that there is an object blocking the descent of the barrier and the motors overload alarm buzzer is activated while either the front or rear motor overload alarm light is turned on in order to request the driver to go outside and check what is blocking the barrier from being lowered. Once the barriers are lowered, and there is snow on the road according to switch (52), the infrared sensor shutters are activated in order to expose the infrared detectors (30) to the field of view in front of barriers (22 and 22'). The shutters provide a means to prevent the lens of the infrared detectors from becoming clouded by dust or soiled water or ice. Should there be then an object detected in front of the barriers by the infrared sensors, the appropriate front or rear barrier infrared sensor alarm light will be turned on along with the alarm buzzer to indicate that a potentially dangerous situation has occurred. In the absence of snow and when the snow on road switch is turned off, the infrared sensor shutters remain closed and the front and rear barrier pressure sensors are read in order to determine if an object has struck one of the barriers (22 or 22'). In such case, the appropriate front or rear barrier pressure sensor alarm light is turned on and the alarm buzzer is also activated. This process of reading the appropriate sensor (30 or 45) depending on the state of the switch (52) continues until distance meter (60) indicates that the appropriate distance has been travelled, at which time the PLC signals the front and rear motor timers to raise the front and rear motors (42) until fully retracted.

Of course, it is possible to replace the various alarm lights and indicator lights illustrated in the block diagram of FIG. 11 by an appropriate display, such as an LCD or LED character display for displaying appropriate messages as set by the PLC (Programmable Logic Controller).

In the preferred embodiment, the first sensing means comprise a pressure transducer (45) provided in the barrier to detect when the barrier (22,22') flexes as a result of being pushed. Of course, pressure can be detected in other ways such as measuring barrier deflection or acoustic coupling and detecting means. The first sensing means may also comprise other detecting means which can work effectively in a given range of climate conditions, such that the combination of the infrared with the first sensing means covers the full range of climate conditions. For example, in the absence of snow, other conventional detection systems may be effectively adapted to work with the safety barrier (22,22'). Ultrasound transceiver systems, microwave transceiver systems, laser beam interrupt systems, are examples of systems which may be adapted to work with the safety barrier (22,22').

In the preferred embodiment, the snow switch (52) causes disabling of the infrared detection (30) when there is no snow. Alternatively, there can be provided a temperature probe to measure the outdoor ambient

temperature to disable the infrared system at elevated outdoor temperatures when the detection could become unreliable. In this way, both the first sensing means and the infrared sensing means could operate over a given intermediate range of weather conditions.

What is claimed is:

1. A vehicle wheel safety barrier system comprising: a barrier member for blocking an object from reaching at least one wheel of the vehicle as the vehicle is moving;  
motor mount means for raising and lowering the barrier member, and for connecting the barrier member to a frame of the vehicle;  
first sensing means for detecting when an object comes in contact with the barrier member and for producing a first output signal in response to the presence of an object;  
infrared sensing means for detecting infrared radiation in a zone in front of the barrier member and for producing an infrared output signal in response to the presence of an object;  
selecting means for providing a climate condition signal indicative of at least a first and second weather condition outside the vehicle; and  
means for generating a warning alarm when the barrier member is lowered, as a function of the climate condition signal wherein said generating means is responsive to the infrared output signal of the infrared sensing means when the first weather condition is selected and said generating means is responsive to the first sensing means when the second weather condition is selection.
2. The barrier system as claimed in claim 1, wherein said first sensing means is pressure sensing means.
3. The barrier system as claimed in claim 2, wherein said first sensing means comprise a pressure transducer for generating said first output signal in a response to an object contacting said barrier member.
4. The barrier system as claimed in claim 1, wherein the first weather condition comprises the presence of snow proximate the barrier member.
5. The barrier system as claimed in claim 2, wherein the second weather condition comprises the absence of snow proximate the barrier member.
6. The barrier system of claim 1 wherein said generating means is response to the infrared sensing means and the first sensing means when a third weather condition is selected by the selecting means.
7. The barrier system as claimed in claim 1, wherein said motor mount means comprise at least two electric motors each mounted to the frame of the vehicle for driving a pair of threaded shaft, the barrier member connected to said threaded shafts by means of nuts threaded onto said shafts for being raised and lowered by rotation of said shafts, and a gaiter covering each said threaded shaft.
8. The barrier system as claimed in claim 7, wherein a spring connection between said nuts and said barrier member is provided.
9. The barrier system as claimed in claim 7, wherein said first sensing means comprise a pressure transducer for use in generating a signal in response an object contacting said barrier member.
10. The barrier system of claim 1 wherein the selecting means is a switch for manually indicating at least the first and second weather conditions.

\* \* \* \* \*



US005155494A

**United States Patent** [19]

Bryant et al.

[11] Patent Number: **5,155,494**[45] Date of Patent: \* **Oct. 13, 1992**[54] **VEHICLE ANTENNA SYSTEM**[75] Inventors: **Everette T. Bryant; Alex F. Wells;  
David M. Phemister**, all of  
Vancouver, Wash.[73] Assignee: **Larsen Electronics, Inc.**, Vancouver,  
Wash.[\*] Notice: The portion of the term of this patent  
subsequent to Mar. 24, 2009 has been  
disclaimed.[21] Appl. No.: **626,628**[22] Filed: **Dec. 12, 1990****Related U.S. Application Data**[63] Continuation of Ser. No. 447,720, Dec. 8, 1989, Pat.  
No. 5,099,252.[51] Int. Cl.<sup>5</sup> ..... **H01Q 1/32**[52] U.S. Cl. .... **343/713; 343/715**[58] Field of Search ..... **343/711, 713, 715, 720;  
455/272, 292**[56] **References Cited****U.S. PATENT DOCUMENTS**

2,206,820	7/1940	Mydlil	343/745
2,559,613	7/1951	Halstead	343/720
2,829,367	4/1958	Rychlik	343/850
3,364,487	1/1968	Maheux	343/702
3,657,652	4/1972	Smith	343/720
4,001,834	1/1977	Smith	343/754
4,028,704	6/1977	Blass	343/715
4,089,817	5/1978	Kirkendall	343/713
4,238,799	12/1980	Parfitt	343/715
4,621,243	11/1986	Harada	343/715
4,658,259	4/1987	Blaese	343/715
4,692,770	9/1987	Kadokura	343/715
4,764,773	8/1988	Larsen et al.	343/713
4,779,098	10/1988	Blaese	343/715
4,794,319	12/1988	Shimazaki	343/711

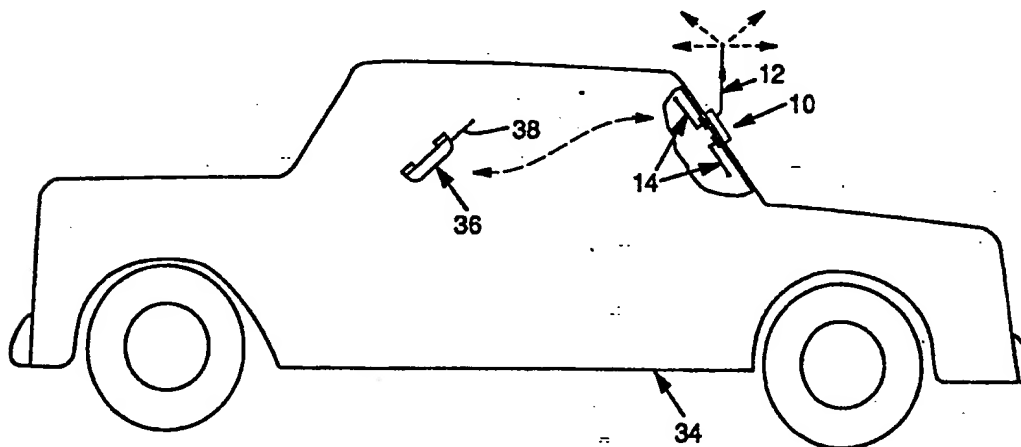
4,804,969	2/1989	Blaese	343/715
4,825,217	4/1989	Young	343/715
4,839,660	6/1989	Hadzoglou	343/715
4,850,035	7/1989	Schiller	455/109
4,862,183	8/1989	Blaese	343/715
5,017,934	5/1991	Blaese	343/713
5,023,622	6/1991	Blaese	343/713

**FOREIGN PATENT DOCUMENTS**

3537107A1	10/1985	Fed. Rep. of Germany	343/715
1203227	8/1958	France	343/715
1227757	6/1959	France	343/715
1-36128	2/1989	Japan	343/711
1-77230	3/1989	Japan	343/711

**OTHER PUBLICATIONS****AARL Handbook for Radio Amateurs**, American  
Radio Relay League, 1991, Ed. 68, pp. 28-34.**Fink, Electronics Engineers' Handbook**, McGraw-Hill  
Book Company, 1st Ed., 1975, p. 3-3.**Johnson, Transmission Lines and Networks**,  
McGraw-Hill Book Company, 1950, p. 239.**Primary Examiner**—Michael C. Wimer  
**Attorney, Agent, or Firm**—Klarquist, Sparkman,  
Campbell, Leigh & Winston[57] **ABSTRACT**

A mobile antenna system features passive repeater operation to transfer energy between a radio transceiver located inside a vehicle and an external radiator mounted on the outside thereof. By this arrangement, a user of the radio transceiver can gain benefit from the external radiator without the hinderance of a physical, wired connection linking the transceiver to the antenna assembly. In a preferred embodiment, the antenna system operates without any electrical cable extending inside the vehicle from the external radiator.

**9 Claims, 2 Drawing Sheets**

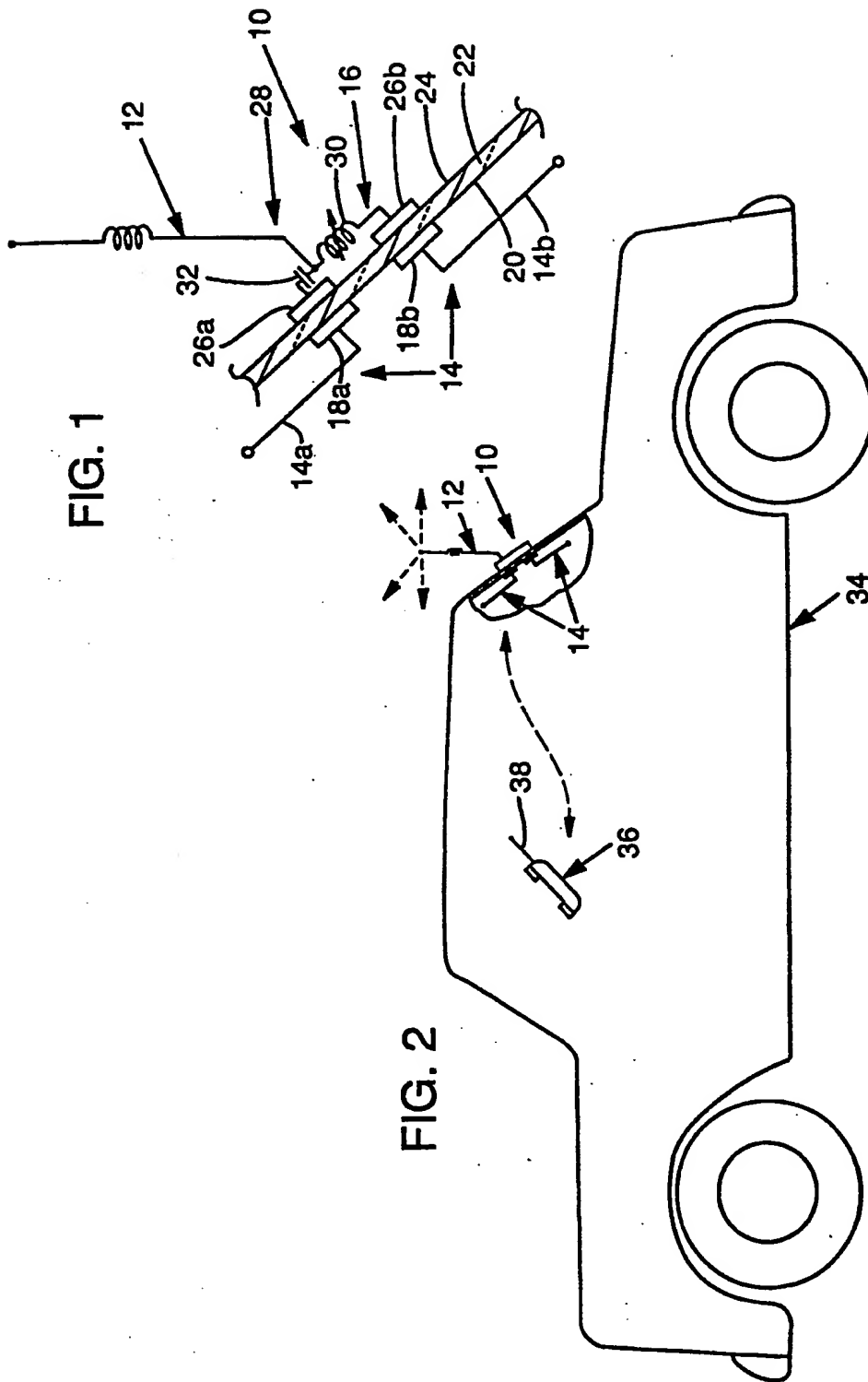


FIG. 3

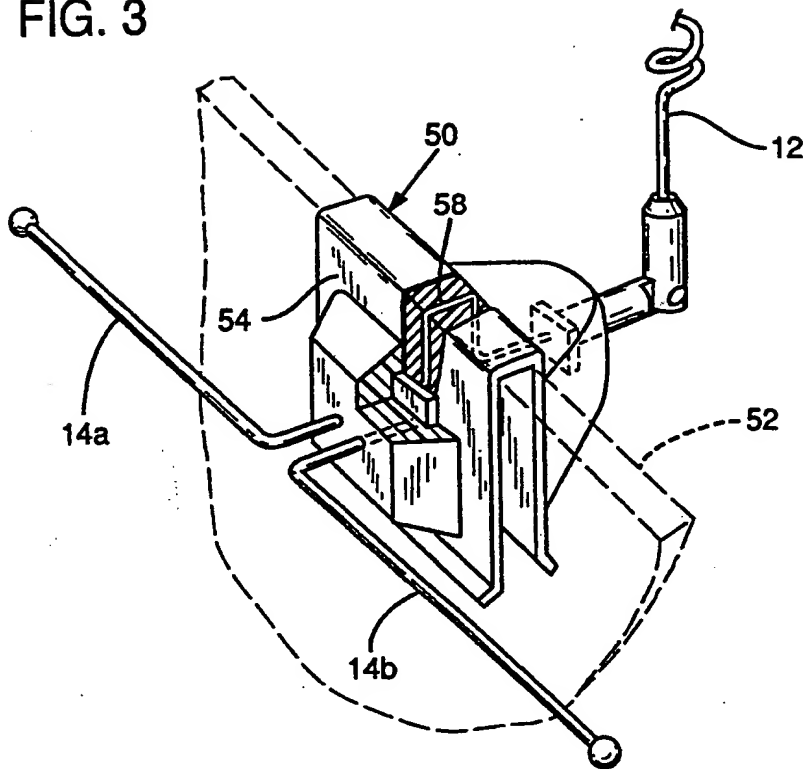
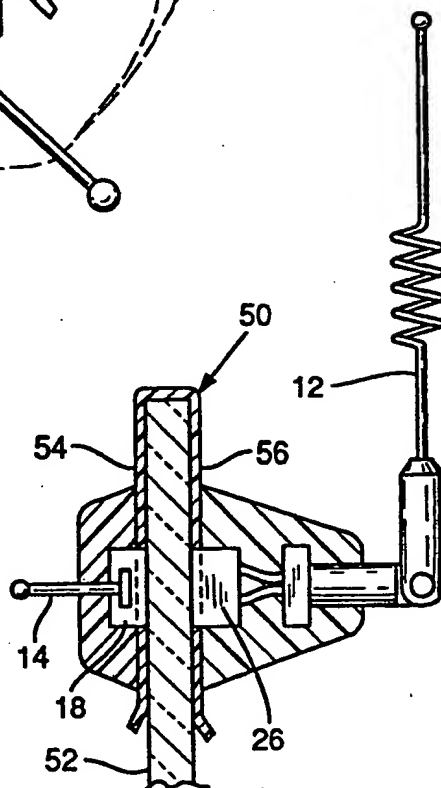


FIG. 4



## VEHICLE ANTENNA SYSTEM

This is a continuation of application Ser. No. 07/447,720, filed Dec. 8, 1989, U.S. Pat. No. 5,099,252.

### FIELD OF THE INVENTION

The present invention relates to the field of cellular telephony, and more particularly relates to mobile antennas used with cellular telephones.

### BACKGROUND AND SUMMARY OF THE INVENTION

Cellular telephony has grown at an exponential rate in recent years. No longer are car phones the exclusive domain of the limousine set. Now they are becoming commonplace in all types of vehicles.

The associated technology has advanced at a dizzying pace as well. No longer are car phones heavy units bolted to the floors of vehicles. Rather, they are now small lightweight units which take a number of forms. So called "mobile" phones usually are permanently installed in a vehicle. These units must be connected to both the vehicle battery and to an external antenna (which is typically mounted on the windshield of the vehicle). "Portable" phones are adapted to be hand carried and include their own battery packs and antennas. A hybrid form of phone, termed a "transportable" can be connected to a vehicle's battery and external antenna, or it may be disconnected and removed from the vehicle, relying on an internal battery pack and its own antenna for operation.

In strong signal areas, all of these units perform well. In fringe areas, however, the associated antennas become more critical. To maintain good communications from a transportable phone at a fringe location, the unit must generally be connected to the vehicle-mounted antenna, rather than rely on its own. If a portable phone is used from a fringe location, it is best to operate the unit outside of the vehicle, with the phone's antenna in the clear. If either a portable or transportable is operated inside the passenger compartment of a vehicle using its built-in antenna, fringe area performance suffers, since the metal surrounding the passenger compartment interferes with transmission of the radio signals.

It will be recognized that it is tedious to connect and disconnect a transportable telephone to a vehicle antenna each time the phone is taken inside or outside a car. However, such action is necessitated in fringe areas. Similarly, it is troublesome for a user of a portable phone to stop the vehicle, get out, and position the portable's own antenna in the clear in order to maintain clear communications. However, this is the present state of the art.

The present invention overcomes these problems. It permits users of transportable and portable telephones to gain the benefit of a vehicle-mounted antenna without requiring that tedious connections be made or broken each time the telephone is moved into or out of a car. The invention even permits portable telephones which have no provision for connection to an external antenna to gain the benefit of an external, vehicle mounted antenna.

In accordance with the present invention, signals are coupled between a vehicle mounted antenna and a cellular telephone by radio rather than by wire. In one embodiment of the invention, this is achieved by pro-

viding an on-glass vehicle antenna with an auxiliary antenna inside the vehicle. Signals are passed to and from the external antenna portion of the on-glass antenna by transmission of signals between the telephone's own antenna and the internal auxiliary antenna portion of the on-glass antenna.

It will be recognized that the invention may be likened to so called "passive repeaters." Such repeaters are known in a number of fields, including relay stations to provide cellular telephone coverage in areas that would otherwise be inaccessible to radio signals, such as inside tunnels. In this application, a high gain antenna, typically a parabolic dish, is mounted outside of the tunnel and is directed towards the nearest cellular broadcasting station. This parabolic antenna is connected by coaxial cable or waveguide to one or more antennas inside the tunnel, thereby providing radio coverage inside the tunnel.

While passive repeaters are a well known technology, no one, to applicants' knowledge, has heretofore applied it to the problem of conveniently using portable and transportable telephones from within the passenger compartments of vehicles. Others skilled in this art failed to arrive at the present invention despite massive research and development efforts in the cellular telephony field by industry leaders in the U.S., Europe and Japan. The nonobviousness of the present invention is illustrated by the unanimity with which it has been overlooked.

The above-described features and advantages of the present invention will be more readily apparent from the following detailed description thereof, which proceeds with reference to the accompanying drawings.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic illustration of an antenna system according to one embodiment of the present invention.

FIG. 2 is a schematic illustration of the antenna system of FIG. 1 used in the passenger compartment of a vehicle in conjunction with a portable cellular telephone.

FIG. 3 is an illustration of an antenna system according to a second embodiment of the present invention.

FIG. 4 is an illustration of an antenna system according to a third embodiment of the present invention.

### DETAILED DESCRIPTION

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the disclosures of U.S. Pat. Nos. 4,862,183, 4,804,969, 4,794,319, 4,764,773 (Larsen), 4,658,259 (Blaese), 4,238,799 (Parfitt), 4,089,817, 4,028,704, 2,829,367 and 2,206,820.

As illustrated by the above-referenced patents, vehicle mounted antennas are typically coupled to the radio transceiver units with which they are used by one of two techniques: direct feed or through-the glass coupling (inductive or capacitive). In direct feed systems, there is an electrical connection from the feed line to the antenna. This connection is usually made by a cable that passes through a hole drilled in the vehicle body. Through-the-glass coupling is most commonly used for cellular vehicle antennas since no hole need be drilled in the vehicle.

Through-the-glass coupling systems usually take one of two forms. In the first, a low impedance presented by the transmission line (connecting to the telephone) is transformed up to match a high impedance presented by

the external antenna. The Larsen and Parfitt patents illustrate this technique. In the Larsen system, the transformation up to the high impedance is performed on the side of the glass outside the vehicle; the through-the-glass coupling is performed at a low impedance. In the Parfitt system, the transformation up to the high impedance is performed on the side of the glass inside the vehicle; the through-the-glass coupling is performed at a high impedance.

In the second type of through-the-glass coupling, a low impedance presented by the transmission line is coupled directly to a low impedance antenna without any impedance transformation. The Blaese patent illustrates this technique.

The present invention is applicable to all of these through-the-glass techniques, as well as to traditional direct feed techniques. For expository convenience, the invention will be illustrated with reference to the Larsen system.

Referring to FIG. 1, an antenna system 10 according to the present invention includes an external radiator 12, an internal auxiliary antenna 14, and some means 16 for coupling energy therebetween. In the illustrated embodiment, the internal auxiliary antenna comprises a dipole dimensioned to present a low resonant impedance in the cellular telephone frequency band. Each leg 14a, 14b of the dipole is connected to an inside capacitive coupling plate 18a, 18b. These inside capacitive coupling plates, in turn, are mounted to an inside surface 20 of a vehicle windshield 22.

On an outside surface 24 of the vehicle windshield 22, opposite the inside coupling plates 18a, 18b, are mounted corresponding outside capacitive coupling plates 26a, 26b. These plates, in turn, are connected to an impedance transformation network 28, which here comprises a series-coupled inductor 30 and capacitor 32. The inductor 30 is tuned to match a high resonant impedance presented by the external radiator 12 to the low impedance coupled through the vehicle windshield from the low impedance internal auxiliary antenna 14.

Referring now to FIG. 2, the antenna 10 of the present invention is shown mounted on the rear windshield of a vehicle 34. Inside the passenger compartment of the vehicle is a portable or transportable telephone 36 with its own antenna 38. Signals broadcast from the telephone antenna 38 are picked up by the internal auxiliary antenna 14 and rebroadcast outside the passenger compartment using the external radiator 12. Similarly, signals received by the external radiator 12 are rebroadcast inside the vehicle by the antenna 14 and received by the telephone antenna 38.

The internal auxiliary antenna may be oriented to achieve vertical or horizontal polarization. Surprisingly, best results are often achieved with horizontal polarization, despite the fact that the telephone antenna with which it is communicating is generally vertically polarized.

In another embodiment of the invention, (FIGS. 3 and 4), the antenna system may be adapted for removable mounting on the top of a vehicle window. A spring-plastic U-shaped clip 50 can slide down over the top edge of a partially-rolled down window 52. The internal auxiliary antenna can be mounted to the inside portion 54 of the clip. The external radiator can be mounted to the outside portion 56 of the clip. Coupling from the internal antenna to the external radiator can be accomplished by a transmission line 58 molded into the plastic clip that connects the two (FIG. 3). Alterna-

tively, a capacitive or inductive coupling arrangement can be used, with one coupling component 26 attached to the outside portion of the clip and the other coupling component 18 attached to the inside portion of the clip (FIG. 4).

It will be recognized that in either of the two foregoing arrangements (i.e. coupling from the internal antenna to the external radiator by a transmission line, or coupling through cooperating components mounted on opposite sides of the glass), no powered circuitry is involved. In other words, the coupling is passive.

If desired, a vehicle may be provided with two or more antenna systems according to the present invention. By using a plurality of such antenna systems, a directional radiation pattern is achieved. Unlike most phased arrays, the directional characteristics here are dependent not only on the spacings of the radiators relative to each other, but also on the location of the portable or transportable telephone's antenna within the array of internal antennas. By moving the telephone within the car, the relative phasings of the signals driving the radiators are altered, changing the net radiation pattern. Thus, by use of a plurality of antenna systems according to the present invention, it is possible to provide a steerable phased array—steerable simply by moving the telephone inside the vehicle.

#### CONCLUSION

It will be recognized that the foregoing embodiments permit transportable phones to gain the benefit of an external vehicle-mounted antenna without having to connect or disconnect the antenna each time the telephone is moved to or from the vehicle. The invention similarly permits portable phones, which often cannot connect to an external antenna even by cable, to easily utilize an external antenna.

Having described and illustrated the principles of our invention with reference to several embodiments thereof, it will be apparent that the invention can be modified in arrangement and detail without departing from such principles. For example, while the invention has been illustrated with reference to an embodiment in which the internal auxiliary antenna is a dipole and presents a low impedance, in other embodiments other interior antenna configurations may be used, some of which present high impedances. Similarly, while the invention has been illustrated with reference to an embodiment in which an inductor/capacitor matching network is used outside the glass, a variety of other matching arrangements may be used on either side of the glass, or no matching network at all may be required. Of course, the invention may also be applied to direct feed antennas by directly connecting the internal auxiliary antenna to the external radiator, as was noted in connection with the second embodiment. Similarly, if a vehicle is provided with a direct feed radiator mounted on the vehicle trunk, an auxiliary antenna may be positioned within the passenger compartment of the vehicle and connected to the external radiator by cabling.

In view of the variety of embodiments to which the principles of our invention may be applied, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Instead, we claim as our invention all such embodiments as may come within the scope and spirit of the following claims and equivalents thereto.

We claim:



1. A method of operating a radio transceiver inside the passenger compartment of a vehicle, the radio transceiver transmitting and receiving signals in a frequency band, the vehicle including a windshield, the method comprising the steps:

when transmitting:

broadcasting a first signal from the transceiver inside the passenger compartment using an antenna connected to the radio transceiver;

receiving the first signal using an internal auxiliary antenna mounted on an inside surface of the windshield but not connected to the radio transceiver, said internal auxiliary antenna being resonant in the frequency band;

coupling the first signal from the internal auxiliary antenna through the windshield and to an external radiator without an electrical cable extending between the internal antenna and the external radiator, the external radiator being mounted on an outside surface of the windshield, the external radiator being resonant in the frequency band; and  
reradiating the first signal from the external radiator;

and  
when receiving:

receiving a second signal using the external radiator; coupling the second signal from the external radiator through the windshield and to the internal antenna without an electrical cable extending between the external radiator and the internal antenna;

reradiating the second signal inside the passenger compartment using the internal auxiliary antenna; and

receiving the reradiated second signal using the antenna connected to the radio transceiver.

2. The method of claim 1 in which the coupling steps each includes capacitively coupling a signal between the internal auxiliary antenna and the external radiator and through the windshield without an electrical cable extending therebetween.

3. A method of operating a cellular telephone inside the passenger compartment of a vehicle, the cellular telephone transmitting signals to and receiving signals from a cellular system, the method comprising the steps:

when transmitting:

broadcasting a first signal from the telephone inside the passenger compartment using an antenna connected to the cellular telephone;

receiving the first signal using an internal auxiliary antenna located inside the passenger compartment but not connected to the cellular telephone, the internal antenna being tuned for resonance in the cellular telephone frequency band;

coupling the first signal from the internal auxiliary antenna and to an external radiator through an insulating material extending therebetween and without an electrical cable extending between the external radiator and the internal auxiliary antenna, the external radiator being tuned for resonance in the cellular telephone frequency band; and  
reradiating the first signal from the external radiator to the cellular system; and

when receiving:

receiving a second signal from the cellular system using the external radiator;

coupling the second signal from the external radiator and to the internal auxiliary antenna through the insulating material extending therebetween and

without an electrical cable extending between the external radiator and the internal auxiliary antenna; reradiating the second signal inside the passenger compartment using the internal auxiliary antenna; and

receiving the reradiated second signal using the antenna connected to the cellular telephone.

4. A vehicle mounted antenna system for use with a cellular telephone comprising:

an external radiator tuned for operation in the cellular telephone frequency band for mounting on the exterior of a vehicle;

means adapted for mounting the radiator on a first surface of an insulating glass window associated with the exterior of the vehicle; and

an internal auxiliary antenna for mounting in a passenger compartment of the vehicle, said internal auxiliary antenna being coupled to the external radiator through the insulating glass window without an electrical cable extending therebetween;

wherein no wired connection links the antenna system with the cellular telephone with which it is used.

5. The antenna system of claim 4 in which the external radiator is oriented vertically and the internal auxiliary antenna is oriented horizontally.

6. An antenna assembly adapted for mounting on a glass surface of a motor vehicle and adapted for use with a portable cellular telephone, characterized by:

an external radiator positioned outside the vehicle and resonant in the cellular telephone frequency band;

an auxiliary radiator coupled with the external radiator;

the absence of a feedline coupling said antenna assembly with the portable cellular telephone with which it is to be used; and

the absence of a feedline coupling the external radiator to the auxiliary radiator;

wherein a user of the portable cellular telephone can gain benefit from the external radiator without the hindrance of a physical, wired connection between the telephone and the antenna assembly.

7. In a method of transmitting cellular telephone signals using a portable cellular telephone and a vehicle mounted antenna assembly, the portable cellular telephone being positioned inside a vehicle, the vehicle mounted antenna assembly including an external radiator that is positioned outside the vehicle and is mounted on an exterior glass surface thereof, the method including coupling cellular telephone signals to the external radiator from the portable cellular telephone, an improvement comprising:

coupling the cellular telephone signals to the antenna assembly from the portable cellular telephone through an auxiliary antenna coupled to the external radiator, without an electrical cable extending between the portable cellular telephone and the antenna assembly, and without an electrical cable extending from the external radiator to inside the vehicle, wherein a user of the portable cellular telephone can gain benefit from the antenna assembly without the hindrance of a physical, wired connection between the telephone and the antenna assembly, and wherein no wired connection needs to be established from the external radiator to inside the vehicle.

8. The method of claim 7 which further includes:

7

providing an internal auxiliary antenna, said internal  
auxiliary antenna being resonant in the cellular  
telephone frequency band;  
positioning the internal auxiliary antenna inside the 5  
vehicle;  
coupling cellular telephone signals to the internal  
auxiliary antenna from an antenna of the cellular  
telephone without an electrical cable extending 10

8

between the cellular telephone and the internal  
auxiliary antenna; and  
coupling cellular telephone signals to the external  
radiator from the internal auxiliary antenna with-  
out an electrical cable extending therebetween.  
9. The method of claim 8 in which the coupling of  
cellular telephone signals to the external radiator from  
the internal auxiliary antenna is effected by capacitive  
coupling.

\* \* \* \* \*

15

20

25

30

35

40

45

50

55

60

65